sui generis

E DANS LE
PROCÉDURE
ENTRE
S

Le profilage dans le cadre d'une procédure d'embauche entre particuliers

Une analyse du cadre légal suisse avec un accent sur la portée du droit fondamental à l'autodétermination en matière informationnelle

Myriam Christ

Notes sur la version numérique de ce livre :

- La version numérique (Open Access) est disponible sur le site de la maison d'édition (www.suigeneris-verlag.ch), sur Google Books et directement via le Digital Object Identifier (DOI). Le DOI de ce livre est indiqué dans les mentions légales.
- Tous les articles juridiques ainsi que tous les arrêts de tribunaux et les décisions de l'autorité librement accessibles sont liés dans la version numérique.
- Les auteurs utilisent souvent des liens vers d'autres sources dans leurs manuscrits. Ceux-ci ne sont pas imprimés dans les livres mais sont inclus sous forme d'hyperliens dans la version digitale.
- Les liens permanents sont utilisés pour créer des liens. Il s'agit de liens vers une version archivée des pages web au moment de l'établissement du lien. Les liens sont persistants, c'est-à-dire qu'ils fonctionnent toujours même si la page d'origine n'est plus accessible et leur contenu ne change pas si la page d'origine change.

Myriam Christ

Le profilage dans le cadre d’une procédure d’embauche entre particuliers

Une analyse du cadre légal suisse avec un accent sur la portée du droit fondamental à l’auto-détermination en matière informationnelle

sui generis, Zürich 2023

Avant-propos

La jurisprudence, ainsi que les modifications législatives, sont prises en compte jusqu'à la fin février 2022. Reflet de la complexité de légiférer en matière de protection des données d'une part et de la crise sanitaire qui a dominé les activités de l'administration fédérale pendant deux ans d'autre part, la révision de l'Ordonnance relative à la Loi sur la protection des données (aOLPD) a pris du retard. Ainsi, cette contribution comprend une analyse du cadre légal prévu par la Loi fédérale sur la protection des données (LPD) adoptée le 25 septembre 2020, qui entrera en vigueur le 1er septembre 2023. En revanche, les quelques modifications apportées par l'Ordonnance sur la protection des données adoptée le 31 août 2022 (OPDo) venant remplacer l'aOLPD n'ont pu être prises en compte que de manière ponctuelle. Cela étant, force est de constater que ces modifications n'ont pas un impact significatif sur l'analyse qui suit. Afin de faciliter la compréhension des propos avancés, une tabelle comparant les dispositions de l'ancienne LPD avec celles qui figurent dans la nouvelle LPD se trouve à la toute fin de cette contribution.

Dans le but de rendre le texte plus fluide, je me suis efforcée de traduire les publications germanophones et anglophones citées (« [traduction] »). Toutefois, ne maîtrisant pas l'art de la traduction, j'invite la lectrice ou le lecteur qui aurait un doute quant à la pertinence d'une citation traduite à consulter le texte dans sa version originale.

Par ailleurs, je tiens à préciser que jusqu'à la fin août 2021, j'ai travaillé en tant que collaboratrice scientifique auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT). Dans cette fonction, j'ai, entre autres, traité les dossiers liés aux traitements de données effectués sur le lieu de travail. Si cette expérience professionnelle a indéniablement influencé l'analyse qui suit, les positions défendues dans le cadre de cette contribution ne reflètent pas la position officielle de cette autorité de surveillance.

Enfin, cette thèse n'aurait pas pu voir le jour sans le soutien précieux de plusieurs personnes.

Je tiens avant tout à remercier Mme Helen Keller, Professeure à l'Université de Zurich et ancienne juge élue au titre de la Suisse à la Cour européenne des droits de l'homme (Cour EDH), qui m'a encadrée tout au long de cette thèse et qui, malgré ses diverses obligations, a toujours répondu à mes questions en un temps record. Qu'elle soit aussi remerciée de m'avoir initiée au fonctionnement de la Cour EDH, de m'avoir laissé toute liberté quant au choix du sujet et à la gestion de ma thèse et de m'avoir, à plusieurs reprises, encouragée à adopter une approche tant théorique que pratique aux défis juridiques de notre époque.

Je remercie également Mme Regina Kiener, Professeure à l'Université de Zurich, qui, malgré son agenda chargé, a accepté d'être rapporteur de cette thèse rédigée en français.

Je remercie toute l'équipe de la maison d'édition *sui generis*, et tout particulièrement Simone Walser, Patricia Michel et Jean Perrenoud pour leur disponibilité et leurs encouragements tout au long du processus de publication. Je tiens également à exprimer ma gratitude envers le Fonds national suisse d'avoir si généreusement pris en charge les frais de publication.

Je tiens aussi à remercier tous les doctorantes et doctorants à l'Université de Zurich qui ont croisé mon chemin entre le 1er septembre 2018 et le 31 janvier 2020 et qui m'ont glissé un mot encourageant au cours d'une pause-café ou à la fin d'un « entraînement ASVZ ». Ayant rédigé sa thèse en même temps que moi, je tiens tout particulièrement à remercier Meret Rehmann pour ses précieux conseils et ses signes d'amitié.

J'exprime également ma gratitude aux collaboratrices et collaborateurs du PFPDT avec qui j'ai eu la chance d'échanger entre le 1er mars 2020 et le 31 août 2021 au sujet de thématiques qui me tiennent à cœur, notamment à Chloé Gay-Balmaz qui m'a initiée au droit de la protection des données avec une rigueur juridique exceptionnelle, à Annina Keller qui m'a rappelé à plusieurs reprises de ne pas oublier la partie faible au contrat de travail, à Anne-Sophie Morand qui a établi le contact avec le think tank *Reatch* ainsi qu'à Selma Duc et Fabiane Midori Sousa Nakagawa qui ont pris le temps de m'expliquer plusieurs notions et qui n'ont cessé de me recommander d'intéressantes publications. Je tiens aussi à remercier les citoyennes et citoyens suisses qui, jour après jour, se sont adressés au service de conseil téléphonique du PFPDT et qui, sans me connaître, m'ont confié leurs questions, parfois très personnelles. Ces échanges téléphoniques ont indéniablement influencé les réflexions ci-après.

Dans une veine plus personnelle, je tiens à remercier mes parents d'avoir financé mes études jusqu'à l'obtention de mon master ainsi que mon stage à la Cour EDH. Mon grand-père, quant à lui, a contribué au financement d'une partie de mes charges durant les sept mois, que j'ai entièrement dédiés à la rédaction de ma thèse. Qu'ils soient remerciés pour leur générosité.

Plusieurs personnes m'ont encouragée lors de moments clés : Tuukka Vähätalo m'a incitée à saisir la chance de rédiger une thèse sous la supervision de Mme la Professeure Keller à la suite de mon stage à la Cour EDH, Dorothea Christ a su trouver les bons mots au bon moment, notamment lorsque je craignais me noyer dans une mer de détails qui devaient encore être abordés avant la date limite de remise, Anna-Lisa Jepsen m'a approvisionnée en sucre pendant les derniers jours de rédaction alors qu'elle était elle-même submergée de travail, et, *last but certainly not least*, Adrienne Enz, ma colocataire à Zurich, a su,

pendant deux ans, marier humour et bienveillance à mon retour de la bibliothèque. Qu'ils soient chaleureusement remerciés pour leur soutien.

Enfin et surtout, j'adresse mes remerciements les plus sincères à Baptiste Pasquier. Au-delà d'avoir cru en l'achèvement de ma thèse depuis notre première discussion y relative, il m'est impossible d'oublier, qu'au tout début du *lockdown*, il s'est assis à côté de moi un matin et a attendu jusqu'à ce que je rédige la première phrase de ce scripte, ce qui m'a permis de prendre confiance et de me lancer dans la rédaction. Sans sa bienveillance, son sens de l'humour et son excellente maîtrise du « principe de proportionnalité » (capacité de garder le recul nécessaire dans les situations les plus diverses), cette thèse n'aurait sans nul doute pas vu le jour sous cette forme.

Biel/Bienne en mars 2023
Myriam Christ

Sommaire

Table des matières

Liste des abréviations

a contrario	latin pour « au contraire »
a fortiori	latin pour « à plus forte raison »
al.	alinéa
aLAGH	ancienne Loi fédérale sur l’analyse génétique humaine du 8 octobre 2004, RS 810.12 (abrogation fixée au 1er décembre 2022)
aLPD	ancienne Loi fédérale sur la protection des données du 19 juin 1992, RS 235.1 (abrogation fixée au 1er septembre 2023)
AOC	appellation d’origine contrôlée
aOCPD	ancienne Ordonnance sur les certifications en matière de protection des données du 28 septembre 2007, RS 235.13 (abrogation fixée au 1er septembre 2023)
aOLPD	ancienne Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993, RS 235.11 (abrogation fixée au 1er septembre 2023)
art.	article
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
BVerfGE	Entscheidungen des [deutschen] Bundesverfassungsgerichts, allemand pour « arrêts du Tribunal constitutionnel fédéral d’Allemagne »
c.	contre
CC	Code civil suisse du 10 décembre 1907, RS 210
CE	Communautés européennes
CEDH	Convention de sauvegarde des droits de l’homme et des libertés fondamentales du 4 novembre 1950, RS 0.101
CEP	Commission d’enquête parlementaire
CFF	Chemins de fer fédéraux
ch.	chiffre
CJUE	Cour de justice de l’Union européenne
CM	Comité des Ministres (du Conseil de l’Europe)
CO	Loi fédérale complétant le Code civil suisse du 30 mars 1911 (Livre cinquième : Droit des obligations), RS 220
Convention 108	— Convention pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, RS 0.235.1

Convention 108+ — Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données personnelles du 18 mai 2018, RS 0.235.11

Cour EDH	Cour européenne des droits de l'homme
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101

culpa in contrahendo — latin pour « responsabilité précontractuelle »

CV	latin pour « document détaillant le parcours et les compétences acquises d'un individu »
déc.	décision
déf.	définition
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
DPD	Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit Directive sur la protection des données personnelles
DRG	Diagnosis Related Groups, anglais pour « système de classification hospitalier américain »
DUDH	Déclaration universelle des droits de l'homme du 10 décembre 1948
éd.	édition
édit.	éditeur(s)
EEE	Espace économique européen
et al.	latin pour « et autres »
etc.	latin pour « et le reste »
EUR	euro(s)
FF	Feuille fédérale
GC	Grande chambre de la Cour européenne des droits de l'homme
GPS	Global Positioning System, anglais pour « assistant de navigation »
HR	Human Resources, anglais pour « ressources humaines »
IA	intelligence artificielle
idem	latin pour « la même chose »
in	latin pour « dans »
in fine	latin pour « en fin de compte »
infra	latin pour « plus loin/plus bas [dans le texte] »

(adresse) IP	Internet Protocol, anglais pour « protocole internet »
K-Tipp	Schweizer Konsumentenmagazin, magazine alémanique des consommateurs
LAGH	Loi fédérale sur l'analyse génétique humaine du 15 juin 2018, RS 810.12
LEg	Loi fédérale sur l'égalité entre femmes et hommes (Loi sur l'égalité) du 24 mars 1995, RS 151.1
let.	lettre
lex specialis	latin pour « loi spéciale » (qui suit une « loi générale »)
LGBTI	Lesbian, Gay, Bisexual, Transgender, and Intersex, anglais pour « Lesbienne, Gay, Bisexuel, Transgenre et Intersexe »
LHand	Loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (Loi sur l'égalité pour les handicapés) du 13 décembre 2002, RS 151.3
LPD	Loi fédérale sur la protection des données du 25 septembre 2020, RS 235.1 (entrée en vigueur fixée au 1er septembre 2023)
LPers	Loi sur le personnel de la Confédération du 24 mars 2000, RS 172.220.1
LSE	Loi fédérale sur le service de l'emploi et la location de services du 6 octobre 1989, RS 823.11
LTr	Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce (Loi sur le travail) du 13 mars 1964, RS 822.11
mutatis mutandis	latin pour « une fois effectuées les modifications nécessaires »
n	note de bas de page
N	note(s)
n°	numéro
nyob	none of your business, Centre européen pour les droits numériques
NZZ	Neue Zürcher Zeitung, allemand pour « Nouvelle Gazette de Zurich »
OAMal	Ordonnance sur l'assurance-maladie du 27 juin 1995, RS 832.102
OCDE	Organisation de coopération et de développement économiques
OCPD	Ordonnance sur les certifications en matière de protection des données du 31 août 2022, RS 235.13 (entrée en vigueur fixée au 1er septembre 2023)
OFJ	Office fédéral de la justice

OHand	Ordonnance sur l'élimination des inégalités frappant les personnes handicapées (Ordonnance sur l'égalité pour les handicapés) du 19 novembre 2003, RS 151.31
OLT 1	Ordonnance 1 relative à la loi sur le travail du 10 mai 2000, RS 822.111
OLT 3	Ordonnance 3 relative à la loi sur le travail (Protection de la santé) du 18 août 1993, RS 822.113
ONG	Organisation non-gouvernementale
ONU	Organisation des Nations Unies
OPDC	Ordonnance concernant la protection des données personnelles du personnel de la Confédération du 22 novembre 2017, RS 172.220.111.4
OPDo	Ordonnance sur la protection des données du 31 août 2022, RS 235.11 (entrée en vigueur fixée au 1er septembre 2023)
OSE	Ordonnance sur le service de l'emploi et la location de services (Ordonnance sur le service de l'emploi) du 16 janvier 1991, RS 823.111
p.	page
PA	Loi fédérale sur la procédure administrative du 20 décembre 1968, RS 172.021
Pacte ONU-II	Pacte international relatif aux droits civils et politiques du 16 décembre 1966, RS 0.103.2
p. ex.	par exemple
PFPDT	Préposé fédéral à la protection des données et à la transparence
PJA	Pratique juridique actuelle
PLR	Parti libéral-radical
PME	petites et moyennes entreprises
PNR	Passenger Name Record, anglais pour « données des dossiers passagers »
pp.	pages
PRISM	nom de code anglais pour un programme américain de surveillance électronique
privatim	Conférence des Préposé(e)s suisses à la protection des données
pt.	point
ratio legis	latin pour « raison d'être de la loi »

ratione personae — latin pour « compétence personnelle »
ratione temporis — latin pour « compétence temporelle »

RDS	Revue de droit suisse

Rec.	Recommandation (du Comité des Ministres du Conseil de l'Europe)
RGPD	Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit Règlement général sur la protection des données
RH	ressources humaines
RS	Recueil systématique
RTS	Radio Télévision Suisse
s.	suivant(e)
SECO	Secrétariat d'État à l'économie
sic	latin pour « tel que cela a été écrit »
SRF	allemand pour « Radio Télévision Suisse »
ss.	suivant(e)s
STE	Série des traités européens
supra	latin pour « plus haut [dans le texte] »
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TFUE	Traité sur le fonctionnement de l'Union européenne
TUE	Traité sur l'Union européenne
UBS	Union de banques suisses
UCLA	University of California, Los Angeles, anglais pour « Université de Californie à Los Angeles »
UE	Union européenne
vol.	volume

Liste des arrêts et de la législation cités

Arrêts cités

Arrêts du Tribunal fédéral

ATF 113 Ia 1
ATF 113 Ia 257
ATF 120 II 118
ATF 122 IV 139
ATF 130 III 699
ATF 131 III 535
ATF 135 III 405
ATF 136 II 508
ATF 137 II 199
ATF 137 III 487
Arrêt 4A_117/2013 du 31 juillet 2013
Arrêt 6B_1174/2017 du 7 mars 2018
Arrêt 6B_869/2020 du 3 septembre 2020
Arrêt 2C_34/2021 du 30 mai 2022

Arrêts du Tribunal administratif fédéral

Arrêt du TAF A-8028/2008 du 14 janvier 2009, *Mitarbeiter-Check*
Arrêt du TAF A-4232/2015 du 18 avril 2017, *Moneyhouse*
Arrêt du TAF A-3548/2018 du 19 mars 2019, *Helsana+*

Arrêts d'instances cantonales

Tribunal des prud'hommes de Lausanne, Jugement n° T304.021563 du 1er juin 2005
Arbeitsgericht Zürich, 4. Abteilung, Jugement n° AN150017-L du 22 janvier 2016

Cour européenne des droits de l'homme

Cour EDH
- *X. et Y. c. Pays-Bas*, n° 8978/80, 26 mars 1985
- *Leander c. Suède*, n° 9248/81, 26 mars 1987
- *Gaskin c. Royaume-Uni*, n° 10454/83, 7 juillet 1989
- *Niemitz c. Allemagne*, n° 13710/88, 16 décembre 1992

- *Segerstedt-Wiberg et al. c. Suède*, n° 62332/40, 6 juin 2006
- *Stefanou c. Grèce*, n° 2954/04, 22 avril 2010
- *Dubetska et al. c. Ukraine*, n° 30499/03, 10 février 2011
- *Vladimir Vasilyev c. Russie*, n° 28370/05, 10 janvier 2012
- *Fáber c. Hongrie*, n° 40721/08, 24 juillet 2012
- *Suso Musa c. Malte*, n° 42337/12, 23 juillet 2013
- *Dembele c. Suisse*, n° 74010/11, 24 septembre 2013
- *Ciorcan et al. c. Roumanie*, n° 29414/09 et 44841/09, 27 janvier 2015
- *Szabó et Vissy c. Hongrie*, n° 37138/14, 12 janvier 2016
- *Boaca et al. c. Roumanie*, n° 40355/11, 12 janvier 2016
- *Grigoryan et Sergeyeva c. Ukraine*, n° 63409/11, 28 mars 2017
- *Aycaguer c. France*, n° 8806/12, 22 juin 2017
- *López Ribalda et al. c. Espagne*, n° 1874/13 et 8567/13, 9 janvier 2018
- *Ivashchenko c. Russie*, n° 61064/10, 13 février 2018
- *Velecka et al. c. Lituanie*, n° 56998/16, 58761/16, 60072/16 et 72001/16, 26 juin 2019
- *Kurt c. Autriche*, n° 62903/15, 4 juillet 2019
- *Sigurdur Einarsson et al. c. Islande*, n° 39757/15, 4 septembre 2019
- *Pryanishnikov c. Russie*, n° 25047/05, 10 septembre 2019
- *T.K. et S.R. c. Russie*, n° 28492/15 et 49975/15, 19 novembre 2019
- *Khan c. Danemark*, n° 26957/19, 12 janvier 2021
- *Terna c. Italie*, n° 21052/18, 14 janvier 2021
- *Ekimdzhiev et al. c. Bulgarie*, n° 70078/12, 11 janvier 2022
- *Rabczewska c. Pologne*, n° 8257/13, 15 septembre 2022

Cour EDH [déc.]
- *Privacy International et al. c. Royaume-Uni*, n° 46259/16, 4 septembre 2020

Cour EDH [GC]
- *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, 4 décembre 2008
- *Géorgie c. Russie (I)*, n° 13255/07, 3 juillet 2014
- *Barbulescu c. Roumanie*, n° 61496/08, 5 septembre 2017
- *Garib c. Pays-Bas*, n° 43494/09, 6 novembre 2017
- *López Ribalda et al. c. Espagne*, n° 1874/13 et 8567/13, 17 octobre 2019
- *N.D. et N.T. c. Espagne*, n° 8675/15 et 8697/15, 13 février 2020
- *Big Brother Watch et al. c. Royaume-Uni*, n° 58170/13, 62322/14 et 24960/15, 25 mai 2021
- *Centrum För Rättvisa c. Suède*, n° 35252/08, 25 mai 2021
- *Khasanov et Rakhmanov c. Russie*, n° 28492/15 et 49975/15, 29 avril 2022

Cour de justice de l'Union européenne (CJUE)

- 29 janvier 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, C-275-06
- 8 avril 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, C-293/12 et C-594/12
- 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12
- 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, C-362/14 (dit *Schrems I*)
- 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems*, C-311/18 (dit *Schrems II*)
- 27 janvier 2022, *Conclusions de l'avocat général de la Cour*, C-817/19
- 21 juin 2022, *Ligue des droits humains c. Conseil des Ministres*, C-817/19

Décisions judiciaires d'autres tribunaux

BVerfGE 65, 1

Législations citées

Législation suisse

- Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
- Loi fédérale sur le renseignement (LRens) du 25 septembre 2015, RS 121
- Loi fédérale sur l'égalité entre femmes et hommes (LEg) du 24 mars 1995, RS 151.1
- Loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (LHand) du 13 décembre 2002, RS 151.3
- Ordonnance sur l'élimination des inégalités frappant les personnes handicapées (OHand) du 19 novembre 2003, RS 151.31
- Loi sur l'Assemblée fédérale (LParl) du 13 décembre 2002, RS 171.10
- Loi fédérale sur la procédure administrative (PA) du 20 décembre 1968, RS 172.021
- Loi sur le personnel de la Confédération (LPers) du 24 mars 2000, RS 172.220.1
- Ordonnance concernant la protection des données personnelles du personnel de la Confédération (OPDC) du 22 novembre 2017, RS 172.220.111.4
- Code civil suisse du 10 décembre 1907, RS 210
- Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations), RS 220

- ancienne Loi fédérale sur la protection des données (aLPD) du 19 juin 1992, RS 235.1, abrogation fixée au 1er septembre 2023
- ancienne Ordonnance relative à la loi fédérale sur la protection des données (aOLPD) du 14 juin 1993, RS 235.11, abrogation fixée au 1er septembre 2023
- ancienne Ordonnance sur les certifications en matière de protection des données (aOCPD) du 28 septembre 2007, RS 235.13, abrogation fixée au 1er septembre 2023
- Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, RS 235.1
- Ordonnance sur la protection des données (OPDo) du 31 août 2022, RS 235.11
- Ordonnance sur les certifications en matière de protection des données (OCPD) du 31 août 2022, RS 235.13
- Code pénal suisse du 21 décembre 1937, RS 311.0
- ancienne Loi fédérale sur l'analyse génétique humaine (aLAGH) du 8 octobre 2004, RS 810.12, abrogation fixée au 1er décembre 2022
- Loi fédérale sur l'analyse génétique humaine (LAGH) du 15 juin 2018, RS 810.12
- Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce (LTr) du 13 mars 1964, RS 822.11
- Ordonnance 1 relative à la loi sur le travail du 10 mai 2000, RS 822.111
- Ordonnance 3 relative à la loi sur le travail (Protection de la santé) du 18 août 1993, RS 822.113
- Loi fédérale sur le service de l'emploi et la location de services (LSE) du 6 octobre 1989, RS 823.11
- Ordonnance sur le service de l'emploi et la location de services (Ordonnance sur le service de l'emploi, OSE) du 16 janvier 1991, RS 823.111
- Ordonnance sur l'assurance-maladie (OAMal) du 27 juin 1995, RS 832.102

Dispositions internationales

Conseil de l'Europe

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950
- Statut du Conseil de l'Europe et textes à caractère statutaire du 5 mai 1949 (STE n° 1)
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE n° 108)

- Protocole n° 11 à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, portant restructuration du mécanisme de contrôle établi par la Convention du 11 mai 1994 (STE n° 155)
- Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données personnelles du 18 mai 2018 (STE n° 223)

Union européenne

- Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000
- Explications relatives à la Charte des droits fondamentaux de l'Union européenne du 14 décembre 2007
- Traité sur le fonctionnement de l'Union européenne (TFUE) du 26 octobre 2012
- Traité sur l'Union européenne (TUE) du 26 octobre 2012
- Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit Règlement général sur la protection des données
- Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données
- Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

Nations Unies

- Déclaration universelle des droits de l'homme du 10 décembre 1948
- Pacte international relatif aux droits civils et politiques du 16 décembre 1966

Bibliographie

Monographies et articles scientifiques

ABEGG ANDREAS, Commentaire de l'art. 328 CO, pp. 911-919, in: Gauch Peter / Aepli Viktor / Stöckli Hubert (édit.), Präjudizienbuch OR, Die Rechtsprechung des Bundesgerichts (1875-2015), 9e éd., Zurich 2016

AJUNWA IFEOMA / CRAWFORD KATE / SCHULTZ JASON, Limitless Worker Surveillance, California Law Review 2017, pp. 735-776

Année politique suisse / Schweizerische Politik 1989, Centre de recherche de politique suisse / Forschungszentrum für schweizerische Politik à l'Université de Berne (édit.), Berne 1990

ARNING MARIAN ALEXANDER / ROTHKEGEL TOBIAS, Commentaire de l'art. 4 ch. 4 RGPD, pp. 121-124, in: Taeger Jürgen / Gabel Detlev (édit.), DSGVO BDSG, Kommentar, 3ème éd., Francfort-sur-le-Main 2019

ARZT GUNTHER, Commentaire de l'art. 179novies CP, pp. 470-476, in : Maurer Urs / Vogt Nedim Peter (édit.), Kommentar zum Schweizerischen Datenschutzgesetz, Bâle/Francfort-sur-le-Main 1995

AUGSBERG INO, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 580-585, in: von der Groeben Hans / Schwarze Jürgen / Hatje Armin (édit.), Europäisches Unionsrecht, Vertrag über die EU, Vertrag über die Arbeitsweise der EU, 7e éd., Baden-Baden 2015

BACHMANN ROLAND, Remarques préliminaires relatives aux art. 1 à 5 LTr, pp. 16-17, in: Blesi Alfred / Pietruszak Thomas / Wildhaber Isabelle (édit.), Kurzkommentar ArG Arbeitsgesetz, Bâle 2018

BARAK AHARON, Constitutional Human Rights And Private Law, pp. 13-42, in: Friedmann Daniel / Barak-Erez Daphne (édit.), Human Rights in Private Law, Oxford 2001

BELSER EVA MARIA

- **§ 1** Problemstellung, pp. 5-32, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (édit.), Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011
- **§ 2** Entwicklung des Datenschutzes, pp. 33-51, in: Belser Eva Maria /Epiney Astrid / Waldmann Bernhard (édit.), Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011

– **§ 5** Die Kompetenzverteilung zwischen Bund und Kantonen, pp. 298-318, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (édit.), Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011
– **§ 6** Der grundrechtliche Rahmen des Datenschutzes, pp. 319-410, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (édit.), Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011
– Zur rechtlichen **Tragweite des Grundrechts auf Datenschutz**, Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung ?, pp. 19-45, in: Epiney Astrid / Fasnacht Tobias / Blaser Gaëtan (édit.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung / Instruments de mise en œuvre du droit à l'autodétermination en matière informationnelle, Zurich/Bâle/Genève 2013

BENHAMOU YANIV, Mise en œuvre judiciaire du droit d'accès LPD – aspects procéduraux choisis, pp. 77-106, in : Métille Sylvain (édit.), Le droit d'accès, Berne 2021

BERANEK ZANON NICOLE, Big Data und Datensicherheit, pp. 85-116, in : Weber Rolf H. / Thouvenin Florent (édit.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zurich/Bâle/Genève 2014

BERSET BIRCHER VALÉRIE / MEIER ANNE, L'impact du droit international en droit suisse du travail, pp. 601-637, in : Wyler Rémy (édit.), Panorama III en droit du travail, Recueil d'études réalisées par les praticiens, Berne 2017

BESSON SAMANTHA
– Comment **humaniser le droit privé** sans commodifier les droits de l'homme, pp. 1-45, in : Werro Franz (édit.), Droit civil et Convention européenne des droits de l'homme / Zivilrecht und Europäische Menschenrechtskonvention, Zurich/Bâle/Genève 2006
– **Droit constitutionnel européen** : précis de droit et résumés de jurisprudence, 4e éd., Berne 2019

BIAGGINI GIOVANNI, Commentaire de l'art. 13 Cst., pp. 198-210, in : Biaggini Giovanni (édit.), BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, Orell Füssli Kommentar, Zurich 2017

BIGLER-EGGENBERGER MARGRITH, Commentaire de l'art. 8 LEg, pp. 204-213, in : Bigler-Eggenberger Margrith / Kaufmann Claudia (édit.), Kommentar zum Gleichstellungsgesetz, Bâle/Francfort-sur-le-Main 1997

BODIE MATTHEW T. / CHERRY MIRIAM A. / MCCORMICK MARCIA L. / TANG JINTONG, The Law And Policy Of People Analytics, University of Colorado Law Review, vol. 88 (2017), n° 4, pp. 961-1042

BRÜHWILER JÜRG, Einzelarbeitsvertrag, Kommentar zu den Art. 319-343 OR, 3e éd., Bâle 2014

BÜCHI MORITZ / FOSCH-VILLARONGA EDUARD / LUTZ CHRISTOPH / TAMÒ-LARRIEUX AURELIA / VELIDI SHRUTHI / VILJOEN SALOME, The Chilling Effects Of Algorithmic Profiling, Mapping The Issues, avril 2020

BÜHLMANN LUKAS / SCHÜEPP MICHAEL, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Eine kritische Analyse anhand des Helsana+ Urteils, in: Jusletter du 15 mars 2021

CELLINA EVA

- **L'influence des réformes européennes** sur la protection des données en Suisse : questions choisies, pp. 221-242, in : Boillet Véronique / Maiani Francesco / Poltier Etienne / Rietiker Daniel / Wilson Barbara (édit.), L'influence du droit de l'Union européenne et de la Convention européenne des droits de l'homme sur le droit suisse, Genève/Bâle/Zurich 2016
- L'introduction de la notion de « **profilage** », iusMAIL DROIT CIVIL, janvier 2018

CHITTARANJAN GOKUL / BLOM JAN / GATICA-PEREZ DANIEL, Mining Large-Scale Smartphone Data for Personality Studies, Personal and Ubiquitous Computing, vol. 17 (2013), pp. 433-450

CHRISTL WOLFIE / SPIEKERMANN SARAH, Networks Of Control, A Report on Corporate Surveillance, Ditigal Tracking, Big Data & Privacy, Vienne 2016

CUPA BASIL, Rechtsschutz gegen präventive Überwachungsmassnahmen am Beispiel des Nachrichtendienstes des Bundes (NDB), thèse soutenue à la Faculté de droit de l'Université de Zurich, Zurich 2014

CUSTERS BART / URSIC HELENA, Worker Privacy in a Digitalized World Under European Law, Comparative Labour Law & Policy Journal, janvier 2018, pp. 323-344

DAEDELOW ROMY, Beschäftigtendatenschutz und DSGVO, Zeitschrift für Datenrecht und Informationssicherheit digma, 2017, pp. 34-37

DIGGELMANN OLIVER, Commentaire de l'art. 13 Cst., pp. 283-301, in : Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (édit.), Bundesverfassung, Basler Kommentar, Bâle 2015

DIGGELMANN OLIVER / CLEIS MARIA NICOLE, How the Right to Privacy Became a Human Right, Human Rights Law Review, 2014, pp. 441-458

DONATSCH ANDREAS, Commentaire de l'art. 179novies CP, p. 434, in: Donatsch Andreas / Heimgartner Stefan / Isenring Bernhard / Maurer Hans / Riesen-Kupper Marcel / Weder Ulrich (édit.), StGB/JStG Kommentar, Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetmG und AuG/AIG, 20e éd., Zurich 2018

DUBEY JACQUES, Droits fondamentaux, Notion, garantie, restriction et juridiction, vol. 1, Bâle 2018

DUNAND JEAN-PHILIPPE
- Commentaire de l'**art. 328b CO**, pp. 317-355, in: Dunand Jean-Philippe / Mahon Pascal (édit.), Commentaire du contrat de travail, Berne 2013
- L'interdiction de la **discrimination à l'embauche** dans la loi fédérale sur l'égalité (LEg), pp. 35-72, in : Dunand Jean-Philippe / Lempen Karine / Mahon Pascal (édit.), L'égalité entre femmes et hommes dans les relations de travail, 1996-2016 : 20 ans d'application de la LEg, Genève/Zurich/Bâle 2016

DUNAND JEAN-PHILIPPE / MAHON PASCAL / WITZIG AURÉLIEN, Avis de droit sur le champ d'application de la loi sur le travail dans le contexte des nouvelles formes d'emploi induites par les technologies numériques, établi à la demande et sur mandat du Secrétariat d'État à l'économie (SECO), Neuchâtel 2018

DUPORTAIL JUDITH, L'amour sous algorithme, Paris 2019

EGLI LUISA INDRA DOMINIQUE, Social Media im Arbeitsrecht, in: Magister, Editions Weblaw, Berne 2020

EMMEL FRANK
- Commentaire de l'**art. 328 CO**, pp. 92-105, in: Huguenin Claire / Müller-Chen Markus (édit.), Vertragsverhältnisse Teil 2 : Arbeitsvertrag, Werkvertrag, Auftrag, GoA, Bürgschaft, Art. 319-529 OR, Handkommentar zum Schweizer Privatrecht, 3e éd., Zurich 2016
- Commentaire de l'**art. 328b CO**, pp. 106-110, in: Huguenin Claire / Müller-Chen Markus (édit.), Vertragsverhältnisse Teil 2: Arbeitsvertrag, Werkvertrag, Auftrag, GoA, Bürgschaft, Art. 319-529 OR, Handkommentar zum Schweizer Privatrecht, 3e éd., Zurich 2016

EPINEY ASTRID
- **§ 9** Allgemeine Grundsätze, pp. 510-558, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (édit.), Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011

– Zur **Abgrenzung** des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, in: Jusletter du 2 mars 2015

EPINEY ASTRID / FASNACHT TOBIAS, § 11 Rechte Einzelner, pp. 597-638, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (édit.), Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011

EPINEY ASTRID / HOFSTÖTTER BERNHARD / MEIER ANNEKATHRIN / THEUERKAUF SARAH, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen: zur rechtlichen Tragweite der europa- und völkerrechtlichen Vorgaben und ihren Implikationen für die Schweiz, Zurich 2007

EPINEY ASTRID / SCHLEISS YVONNE, § 3 Völkerrecht, pp. 53-118, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Berne 2011

ESSER MARTIN, Commentaire de l'art. 4 ch. 4 RGPD, pp. 98-99, in: Esser Martin / Kramer Philipp / von Lewinski Kai (édit.), DSGVO BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze, 7ème éd., Hürth 2020

EUBANKS VIRGINIA, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, New York 2018

FABBRINI FEDERICO, The EU Charter of Fundamental Rights and the Rights to Data Privacy : the EU Court of Justice As a Human Rights Court, mars 2015

FARNER MARTIN, Introduction à la LTr, pp. 2-14, in: Blesi Alfred / Pietruszak Thomas / Wildhaber Isabelle (édit.), Kurzkommentar ArG Arbeitsgesetz, Bâle 2018

FASNACHT TOBIAS, Die Einwilligung im Datenschutzrecht, Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht, thèse soutenue à la Faculté de droit de l'Université de Fribourg, Zurich 2017

FAVRE CHRISTIAN / MUNOZ CHARLES / TOBLER ROLF A., Le contrat de travail : code des obligations (art. 319-362 CO), loi sur l'égalité, loi sur le travail, loi sur le service de l'emploi et la location de services, Code annoté de la jurisprudence fédérale et cantonale, 2e éd., Lausanne 2010

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 6/2013, pp. 837-864

FOLZ HANS-PETER, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 1120-1121, in: Vedder Christoph / Heintschel von Heinegg Wolff (édit.), Europäisches Unionsrecht, EUV – AEUV – Grundrechte-Charta, Handkommentar mit den vollständigen Texten der Protokolle und Erklärungen und des EAGV, Baden-Baden 2012

FRENKEL SHEERA / KANG CECILIA, Inside Facebook, Die hässliche Wahrheit, Francfort 2021

FROWEIN JOCHEN ABR., Commentaire de l'art. 8 CEDH, pp. 287-317, in : Frowein Jochen Abr. / Peukert Wolfgang (édit.), Europäische Menschenrechtskonvention, EMRK-Kommentar, 3e éd., Kehl-sur-le-Rhin 2009

FÜZESSÉRY SIMONE / SCHNEIDER DANIELLE, La révision de la loi fédérale sur la protection des données, Une comparaison avec le règlement (UE) 2016/679, pp. 139-158, in : Epiney Astrid / Rovelli Sophia (édit.), Datenschutzgrundverordnung (DSGVO) : Tragweite und erste Erfahrungen / Le règlement général sur la protection des données (RGPD) : portée et premières expériences, Zurich/Bâle/Genève 2020

GASSER URS, Perspectives on the Future of Digital Privacy, Revue de droit suisse, 2015, vol. 2, pp. 335-448

GONIN LUC, Droit constitutionnel suisse, Genève/Zurich 2021

GOOLD BENJAMIN, Surveillance and the Political Value of Privacy, Amsterdam Law Forum, vol. 1, n° 4, 2009, pp. 3-6

GRIESINGER MARCEL, Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO, in: Jusletter du 20 janvier 2020

GUTWIRTH SERGE / HILDEBRANDT MIREILLE, Some Caveats on Profiling, pp. 31-41, in: Gutwirth Serge / Poullet Yves / De Hert Paul (édit.), Data Protection in a Profiled World, Pays-Bas 2010

HÄFELIN ULRICH / HALLER WALTER / KELLER HELEN / THURNHERR DANIELA, Schweizerisches Bundesstaatsrecht, 10e éd., Zurich 2020

HANSEN MARIT, Arbeitnehmer: Freiwild der Überwachung ?, Bericht über die Sommerakademie 2009, Datenschutz und Datensicherheit 11/2009, p. 650

HÄUSELMANN ANDREAS NICHOLAS, Profiling and the GDPR: Harmonised Confusion, in: Jusletter du 12 février 2018

HELFRICH MARCUS
- Commentaire de l'art. 4 RGPD, pp. 326-395, in: Sydow Gernot (édit.), Europäische Datenschutzgrundverordnung, Handkommentar, 2e éd., Baden-Baden/Vienne/Zurich 2018
- Commentaire de l'art. 22 RGPD, pp. 659-675, in : Sydow Gernot (édit.), Europäische Datenschutzgrundverordnung, Handkommentar, 2e éd., Baden-Baden/Vienne/Zurich 2018

HERBST TOBIAS / BUCHNER BENEDIKT, Commentaire de l'art. 4 ch. 4 RGPD, pp. 170-172, in : Kühling Jürgen / Buchner Benedikt (édit.), Datenschutz-Grundverordnung BDSG, Kommentar, 3ème éd., Munich 2020

HERTIG RANDALL MAYA / MARQUIS JULIEN, Commentaire de l'art. 13 Cst., pp. 490-518, in: Martenet Vincent / Dubey Jacques (édit.), Constitution fédérale, Commentaire romand, vol. 1er, Bâle 2021

HEUBERGER OLIVIER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, thèse soutenue à la Faculté de droit de l'Université de Lucerne, Lucerne 2020

HILDEBRANDT MIREILLE, Defining Profiling: a New Type of Knowledge ?, pp. 17-30, in: Hildebrandt Mireille / Gutwirth Serge (édit.), Profiling the European Citizen, Cross-Disciplinary Perspectives, Belgique/Pays-Bas 2008

HIRSCH DENNIS D., Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law, Georgia Law Review, vol. 41 (automne 2006), n° 1, pp. 1-63

HUGENTOBLER MARKUS, Commentaire de l'art. 328 CO, pp. 591-602, in: Fischer Willi / Luterbacher Thierry (édit.), Haftpflichtkommentar, Kommentar zu den schweizerischen Haftpflichtbestimmungen, Zurich 2016

JOHLEN HERIBERT, Commentaire de l'art. 8 Charte, pp. 207-223, in: Stern Klaus / Sachs Michael (édit.), Europäische Grundrechte-Charta GRCh, Kommentar, Munich 2016

JÖHRI YVONNE, § 8 Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten, pp. 245-277, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (édit.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Handbücher für die Anwaltspraxis, Bâle 2015

KASPER GABRIEL / WILDHABER ISABELLE, Big Data am Arbeitsplatz, Datenschutz- und arbeitsrechtliche Herausforderungen von People Analytics in Schweizer Unternehmen, pp. 189-232, in: Kieser Ueli / Pärli Kurt / Uttinger Ursula (édit.): Datenschutztagung 2018 – Ein Blick auf aktuelle Rechtsentwicklungen, Zurich 2019

KAUFMANN CHRISTINE / SCHUERCH RES, Digitalisierung und Privatsphäre im Arbeitsverhältnis – Rechtliche Grundlagen und Problemfelder, Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR), **Positionspapier**, août 2019

KAUFMANN CHRISTINE / SCHUERCH RES, **Digitalisierung und Privatsphäre im Arbeitsverhältnis**, Rechtliche Grundlagen und aktuelle Problemfelder, Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR), 1er septembre 2021

KIENER REGINA, § 30 Allgemeine Grundrechtslehren, pp. 460-494, in: Biaggini Giovanni / Gächter Thomas / Kiener Regina (édit.), Staatsrecht, 3e éd., Zurich/ Saint-Gall 2021

KLABUNDE ACHIM, Commentaire de l'art. 4 RGPD, pp. 167-187, in: Ehmann Eugen / Selmayr Martin (édit.), Datenschutz-Grundverordnung, Kommentar, 2e éd., Munich 2018

KNECHT MATTHIAS, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 2222-2224, in: Schwarze Jürgen (édit.), EU-Kommentar, 2e éd., Baden-Baden 2009

KOKOTT JULIANE / SOBOTTA CHRISTOPH, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, vol. 3 (2013), n° 4, pp. 222-228

KOSINSKI MICHAL / WANG YILUN / LAKKARAJU HIMABINDU / LESKOVEC JURE, Mining Big Data to Extract Patterns and Predict Real-Life Outcomes, Psychological Methods, vol. 21 (2016), n° 4, pp. 493-506

KRANENBORG HERKE, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 231-289, in : Peers Steve / Hervey Tamara / Kenner Jeff / Ward Angela (édit.), The EU Charter of Fundamental Rights, A Commentary, 2e éd., Oxford 2021

LEICHT-DEOBALD ULRICH / BUSCH THORSTEN / SCHANK CHRISTOPH / WEIBEL ANTOINETTE / SCHAFHEITLE SIMON / WILDHABER ISABELLE / KASPER GABRIEL, The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity, Journal of Business Ethics, 2019, pp. 377-392

LEMPEN KARINE, Protection des données et discrimination lors de la procédure de recrutement, pp. 270-286, in: Dunand Jean-Philippe/Mahon Pascal (édit.), La protection des données dans les relations de travail, Genève 2017

LOCK TOBIAS, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 2121-2127, in: Kellerbauer Manuel / Klauert Marcus / Tomkin Jonathan (édit.), The EU Treaties and the Charter of Fundamental Rights, A Commentary, Oxford 2019

LOEWE-BAUR MIRJAM, Der Risikoorientierte Sanktionenvollzug (ROS), Ergebnisse und Erkenntnisse einer Evaluation, Zurich 2017

LUBISHTANI KASTRIOT / FLATTET MAXIME, La démocratie directe face à la manipulation de l'information par des particuliers, Ses protections constitutionnelle et pénale, PJA 7/2019, pp. 710-723

LYON DAVID, Surveillance after Snowden, Cambridge (Royaume-Uni) 2015

MALINVERNI GIORGIO / HOTTELIER MICHEL / HERTIG RANDALL MAYA / FLÜCKIGER ALEXANDRE, Droit constitutionnel suisse, vol. 1, 4e éd., Berne 2021

MARSCH NIKOLAUS, Das europäische Datenschutzgrundrecht, Grundlagen – Dimensionen – Verflechtungen, Tubingue 2018

MARTENET VINCENT
- **La protection** contre les discriminations émanant de particuliers, RDS 2006, vol. 1, pp. 419-458
- Commentaire de l'**art. 35 Cst.**, pp. 1021-1051, in: Martenet Vincent / Dubey Jacques (édit), Constitution fédérale, Commentaire romand, vol. 1er, Bâle 2021

MATHIS-ZWYGART ESTELLE, La surveillance des travailleurs sous l'angle des articles 328b CO et 26 OLT 3, pp. 310-324, in: Dunand Jean-Philippe / Mahon Pascal (édit.), La protection des données dans les relations de travail, Genève 2017

MEIER PHILIPPE
- **Protection des données** : fondements, principes généraux et droit privé, Berne 2011
- Le défi de **Big Data** dans les relations entre privés : avec quelques réflexions de lege ferenda, pp. 47-94, in: Epiney Astrid (édit.), Big Data und Datenschutzrecht, Zurich 2016

MÉTILLE SYLVAIN
– **Jurisprudence actuelle** en matière de protection des données, Surveillance, infiltration et transmission de données à un tiers : quelques atteintes à la sphère privée qui ont occupé récemment les tribunaux, pp. 113-124, in: Epiney Astrid / Fasnacht Tobias / Blaser Gaëtan (édit.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung / Instruments de mise en œuvre du droit à l'autodétermination informationnelle, Zurich/Bâle/Genève 2013
– **Internet et droit**, Protection de la personnalité et questions pratiques, Genève/Zurich 2017
– **Le droit au respect de la vie privée:** les défis digitaux, une perspective de droit comparé – Suisse, in: Unité Bibliothèque de droit comparé, Direction générale des services de recherche parlementaire, Secrétariat général du Parlement européen, 2018
– Le traitement de données personnelles sous l'angle de **la (nouvelle) loi fédérale** sur la protection des données, La semaine judiciaire, vol. 143, n° 1 (mars 2021), pp. 1-46

MÉTILLE SYLVAIN / ACKERMANN ANNELISE, RGPD : application territoriale et extraterritoriale, pp. 77-97, in: Epiney Astrid (édit.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen / Le règlement général sur la protection des données (RGPD) : portée et premières expériences, Zurich 2020

MÉTILLE SYLVAIN / RAEDLER DAVID, Révision de la LPD : des sanctions à contre-courant et à contre-raison, Plaidoyer 02/2017, pp. 38-43

MÉTILLE SYLVAIN / XUAN NADJA NGUYEN, Un profil de personnalité n'est pas nécessaire pour juger de la solvabilité d'une personne, Arrêt du Tribunal administratif fédéral du 18 avril 2017 (A-4232/2015), Medialex 2017, pp. 176-179

MOECKLI DANIEL, Persönlichkeitsschutz, pp. 1383-1411, in: Diggelmann Oliver / Hertig Randall Maya / Schindler Benjamin (édit.), Verfassungsrecht der Schweiz, vol. 2, Zurich 2020

MÖHLE JAN-PETER, Totalrevision des Schweizer Datenschutzgesetzes – Ende gut, alles gut?, in: Datenschutz und Datensicherheit 9/2021, pp. 598-602

MONTAVON MICHAEL, Cyberadministration et protection des données : étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, thèse soutenue à la Faculté de droit de l'Université de Fribourg, Genève/Zurich/Bâle 2021

MONTJOYE YVES-ALEXANDRE / HIDALGO CÉSAR A. / VERLEYSEN MICHEL / BLONDEL VINCENT D., Unique in the Crowd: the Privacy Bounds of Human Mobility, Scientific Reports 3, 2013

MORGENROTH MARKUS, Sie kennen dich ! Sie haben dich! Sie steuern dich! Die wahre Macht der Datensammler, Munich 2016

MÜLLER ROLAND A. / MADUZ CHRISTIAN, Commentaire de l'art. 1er LTr, pp. 32-37, in: Müller Roland A. / Maduz Christian (édit.), ArG Kommentar, Arbeitsgesetz mit weiteren Erlassen im Bereich Arbeitsschutz, Orell Füssli Kommentar, 8e éd., Zurich 2017

MUND CLAUDIA, Grundrechtsschutz und genetische Information, Postnatale genetische Untersuchungen im Lichte des Grundrechtsschutzes unter besonderer Berücksichtigung genetischer Untersuchungen im Arbeits- und Versicherungsbereich, thèse soutenue à la Faculté de droit de l'Université de Bâle, Bâle/Genève/Munich 2005

NAGUIB TAREK, « Racial Profiling » – Definitionen und Einordnung, in: Jusletter du 18 septembre 2017

NIANG FATIMA, De quelques contraintes en droit européen et international, pp. 193-208, in: Besson Samantha / Ziegler Andreas (édit.), Le juge en droit européen et international, Zurich 2013

NIKLAS THOMAS / THURN LUKAS, Arbeitswelt 4.0 – Big Data im Betrieb, Betriebs-Berater 2017, pp. 1589-1596

NÖTZLI HARRY, Commentaire de l'art. 6 LTr, pp. 86-100, in: Blesi Alfred / Pietruszak Thomas / Wildhaber Isabelle (édit.), Kurzkommentar ArG, Arbeitsgesetz, Bâle 2018

NOUREDDINE HUSSEIN, § 3 Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, V. Besondere Bestimmungen der Datenbearbeitung durch Privatpersonen, pp. 98-108, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (édit.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Handbücher für die Anwaltspraxis, Bâle 2015

OHM PAUL, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review 2010, pp. 1701-1777

O'NEIL CATHY, Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy, New York 2016

PÄRLI KURT, Commentaire de l'art. 328b CO, pp. 409-423, in: Baeriswyl Bruno / Pärli Kurt (édit.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, Berne 2015

PASQUALE FRANK, The Black Box Society, The Secret Algorithms That Control Money and Information, Cambridge (MA) 2016

PELLASCIO MICHEL
- Commentaire de l'**art. 328 CO**, pp. 845-852, in: Kren Kostkiewicz Jolanta / Wolf Stephan / Amstutz Marc / Fankhauser Roland (édit.), OR Kommentar, Schweizeriches Obligationenrecht, Orell Füssli Kommentar, 3e éd., Zurich 2016
- Commentaire de l'**art. 328b CO**, pp. 854-857, in: Kren Kostkiewicz Jolanta / Wolf Stephan / Amstutz Marc / Fankhauser Roland, OR Kommentar, Schweizeriches Obligationenrecht, Orell Füssli Kommentar, 3e éd., Zurich 2016

PÉTERMANN NATHANAËL, Les obligations positives de l'État dans la jurisprudence de la Cour européenne des droits de l'homme, Théorie générale, incidences législatives et mise en œuvre en droit suisse, thèse soutenue à la Faculté de droit, des sciences criminelles et d'administration publique de l'Université de Lausanne, Berne 2014

PODESTA JOHN / PRITZKER PENNY / MONIZ ERNEST (et al.), Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, Rapport du 1er mai 2014

POULLET YVES, Towards an Ethical Development of AI Systems, Some Thoughts on the Draft Report Containing the « Proposal For A Resolution From The European Parliament (sic) Containing Recommandations to the Commission Concerning a Framework of Ethical Aspects in Artificial Intelligence, Robotics and Related Technologies (2020/2012 (INL)) », pp. 138-143, in: Université de Fribourg, L'intelligence artificielle et protection des données, 13e Journée suisse de droit de la protection des données, 2 octobre 2020

POWELL JULIAN, Die Revision der kantonalen Datenschutzgesetze, Unter Berücksichtigung der Rechtsentwicklungen in Europa und auf Bundesebene, in: Jusletter du 31 mai 2021

PRANTL HERIBERT, Weltweiter Datenschutz und zukünftiger Schutz der Grundrechte, Datenschutz und Datensicherheit 6/2016, pp. 347-353

PROBST THOMAS, Die Verknüpfung von Personendaten und deren rechtliche Tragweite, pp. 1-40, in: Epiney Astrid / Probst Thomas / Gammenthaler Nina (édit.), Datenverknüpfung, Problematik und rechtlicher Rahmen / L'interconnexion des données, Problématiques et cadre juridique, Zurich 2011

PULVER BERNHARD, Die Verbindlichkeit staatlicher Schutzpflichten – am Beispiel des Arbeitsrechts, PJA 4/2005, pp. 413-423

REHBINDER MANFRED / STÖCKLI JEAN-FRITZ, Commentaire de l'art. 328b CO, pp. 487-496, in: Hausheer Heinz / Walter Hans Peter (édit.), Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Die einzelnen Vertragsverhältnisse, Der Arbeitsvertrag, Art. 319-362 OR, Berner Kommentar, Berne 2010

REHM GEBHARD MARC
- Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law, 23 janvier 2000
- Privacy in the **Digital Age**: Vanishing into Cyberspace?, pp. 373-387, in: Friedmann Daniel / Barak-Erez Daphne (édit.), Human Rights in Private Law, Oxford 2001

REIMER PHILIPP, Commentaire de l'art. 5 RGPD, pp. 396-412, in: Sydow Gernot (édit.), Europäische Datenschutzgrundverordnung, Handkommentar, 2e éd., Baden-Baden 2018

REINSCH ROGER W. / GOLTZ SONIA, The Law and Business of People Analytics: Can the Attempt to Be More Discriminating Be More Discriminatory Instead?, Saint Louis University Law Journal, 2016, pp. 35-63

RIEMER-KAFKA GABRIELA / UEBERSCHLAG JAKOB, Commentaire de l'art. 8 LEg, pp. 274-290, in: Kaufmann Claudia / Steiger-Sackmann Sabine (édit.), Kommentar zum Gleichstellungsgesetz, 2e éd., Bâle 2009

RIESZ THOMAS, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 155-225, in: Holoubek Michael / Lienbacher Georg (édit.), Charta der Grundrechte der Europäischen Union, GRC-Kommentar, 2e éd., Vienne 2019

ROSENTHAL DAVID
- Commentaire de l'**art. 4 LPD**, pp. 76-123, in: Rosenthal David / Jöhri Yvonne (édit.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zurich 2008

– Der **Entwurf** für ein neues Datenschutzgesetz, Was uns erwartet und was noch zu korrigieren ist, in: Jusletter du 27 novembre 2017
– **Das neue Datenschutzgesetz**, in: Jusletter du 16 novembre 2020

ROUVROY ANTOINETTE, « Of Data and Men », Fundamental Rights and Freedoms in a World of Big Data, Strasbourg 2016

RUDOLPH ROGER
– **Stellenbewerbung und Datenschutz**, thèse soutenue à la Faculté de droit de l'Université de Zurich, Zurich 1997
– **Richterliche Rechtsfindung** im Arbeitsrecht, Zurich 2021

SAMOCHOWIEC JAKUB/MÜLLER ANDREAS, La montre connectée nuit-elle à la solidarité ?, Scénarios pour un système de santé basé sur les données, novembre 2021

SCHEFER MARKUS, Grundrechtliche Schutzpflichten und die Auslagerung staatlicher Aufgaben, PJA 10/2002, pp. 1131-1143

SCHMIDT KIRSTEN JOHANNA, Datenschutz als Vermögensrecht: Datenschutzrecht als Instrument des Datenhandels, Wiesbaden 2020

SCHOLZ PHILIP
– Commentaire de l'**art. 4 ch. 4 RGPD**, pp. 307-311, in: Simitis Spiros / Hornung Gerrit / Spiecker genannt Döhmann Indra (édit.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2020
– Commentaire de l'**art. 22 RGPD**, pp. 704-723, in: Simitis Spiros / Hornung Gerrit / Spiecker genannt Döhmann Indra (édit.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2020

SCHREIBER LUTZ, Commentaire de l'art. 4 ch. 4 RGPD, p. 36, in: Plath Kai-Uwe (édit.), DSGVO / BDSG, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3ème éd., Cologne 2018

SCHWARTMANN ROLF / HERMANN MAXIMILIAN, Commentaire de l'art. 4 ch. 4 RGPD, pp. 48-50, in : Schwartmann Rolf / Jaspers Andreas / Thüsing Gregor / Kugelmann Dieter (édit.), DS-GVO / BDSG, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Heidelberg 2018

SCHWEIZER ALEX, Data Mining, Data Warehousing, Datenschutzrechtliche Orientierungshilfen für Privatunternehmen, Zurich 1999

SCHWEIZER RAINER J.
– Die **Rechtsprechung des E**uropäischen **G**erichtshofes für **M**enschenrechte zum Persönlichkeits- und Datenschutz, Datenschutz und Datensicherheit 8/2009, pp. 462-468

– Commentaire de l'**art. 13 al. 2 Cst.**, pp. 367-377, in: Ehrenzeller Bernhard / Schindler Benjamin / Schweizer Rainer J. / Vallender Klaus A. (édit.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3[e] éd, Zurich/ Saint-Gall 2014

SNYDER TIMOTHY, On Tyranny: Twenty Lessons from the Twentieth Century, Londres 2017

SOLOVE DANIEL J., Nothing to Hide: The False Tradeoff between Privacy and Security, New Haven et Londres 2011

SPIECKER GENANNT DÖHMANN INDRA, Profiling, Big Data, Artificial Intelligence und Social Media – Gefahren für eine Gesellschaft ohne effektiven Datenschutz, pp. 345-372, in: Festschrift für Erich Schweighofer, Berne 2020

STAEHELIN ADRIAN
– Commentaire de l'**art. 320 CO**, pp. 45-69, in: Gauch Peter / Schmid Jörg (édit.), Der Arbeitsvertrag, Art. 319-330a OR, Zürcher Kommentar zum schweizerischen Zivilrecht, 4[e] éd., Zurich 2006
– Commentaire de l'**art. 328 CO**, pp. 370-388, in: Gauch Peter / Schmid Jörg (édit.), Der Arbeitsvertrag, Art. 319-330a OR, Zürcher Kommentar zum schweizerischen Zivilrecht, 4[e] éd., Zurich 2006
– Commentaire de l'**art. 328b CO**, pp. 396-406, in: Gauch Peter / Schmid Jörg (édit.), Der Arbeitsvertrag, Art. 319-330a OR, Zürcher Kommentar zum schweizerischen Zivilrecht, 4[e] éd., Zurich 2006

STENGEL CORNELIA / STÄUBLE LUCA, Vom Persönlichkeitsprofil zum Profiling mit hohem Risiko, Ein Beitrag zur Begriffsabgrenzung im Differenzbereinigungsverfahren für ein totalrevidiertes Datenschutzgesetz, in : Jusletter du 20 janvier 2020

STREINZ RUDOLF, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 2705-2708, in : Streinz Rudolf (édit.), EUV/AEUV, Vertrag über die EU, Vertrag über die Arbeitsweise der EU, Charta der Grundrechte der Europäischen Union, Beck'sche Kurz-Kommentare, vol. 57, 3[e] éd., Munich 2018

STREINZ RUDOLF / MICHL WALTHER, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, Europäische Zeitschrift für Wirtschaftsrecht, novembre 2011, pp. 384-388

SYDOW GERNOT, Commentaire de l'art. 1[er] RGPD, pp. 305-313, in : Sydow Gernot (édit.), Europäische Datenschutzgrundverordnung, Handkommentar, 2[e] éd., Baden-Baden 2018

TAMÒ-LARRIEUX AURELIA, Designing for Privacy and Its Legal Framework : Data Protection by Design and Default for the Internet, thèse soutenue à la Faculté de droit de l'Université de Zurich, Cham 2018

THOUVENIN FLORENT

– Privatversicherungen : Datenschutzrecht als Grenze der **Individualisierung** ?, pp. 15-42, in : Epiney Astrid / Sangsue Déborah (édit.), Datenschutz und Gesundheitsrecht / Protection des données et droit de la santé, Zurich 2019
– **Informations- und Kommunikationsrecht**, Vorlesungsunterlagen im Herbstsemester 2020 am rechtswissenschaftlichen Institut der Universität Zürich

TRECHSEL STEFAN / LIEBER VIKTOR, Commentaire de l'art. 179[novies] CP, pp. 1034-1036, in : Trechsel Stefan / Pieth Mark (édit.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 3[e] éd., Zurich 2018

TRUTMANN VERENA, Zum Persönlichkeitsschutz im Arbeitsrecht, pp. 465-475, in : Böckli Peter / Eichenberger Kurt / Hinderung Hans / Tschudi Hans Peter (édit.), Festschrift für Frank Vischer zum 60. Geburtstag, Zurich 1983

UEBERSCHLAG JAKOB, Repetitorium zum Gleichstellungsgesetz (GlG), Berne 2012

UTTINGER URSULA, Datenschutzüberprüfungen : Zertifizierungen sowie andere Möglichkeiten oder : Was hat Art. 11 DSG verändert, pp. 69-80, in : Kieser Ueli / Pärli Kurt (édit.), Datenschutz im Arbeits-, Versicherungs- und Sozialbereich : Aktuelle Herausforderungen, Saint-Gall 2012

VASELLA DAVID

– Zur Freiwilligkeit und zur Ausdrücklichkeit der **Einwilligung** im Datenschutzrecht, in : Jusletter du 16 novembre 2015
– ArG ZH : OR 328b als eigenständige Verbotsnorm ohne Rechtfertigungsmöglichkeit, 13. Mai 2016
– Zum Entwurf des DSG vom 15. September 2017, walderwyss rechtsanwälte

WACHTER SANDRA / MITTELSTADT BRENT / FLORIDI LUCIANO, Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation, International Data Privacy Law, vol. 7 (2017), n° 2, pp. 76-99

WALTER JEAN-PHILIPPE
– **Le profilage** des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données, pp. 87-114, in : Epiney Astrid / Probst Thomas / Gammenthaler Nina (édit.), Datenverknüpfung : Problematik und rechtlicher Rahmen / L'interconnexion des données : Problématique et cadre juridique, Zurich/Bâle/Genève 2011
– « Vingt ans de législation sur la protection des données, rétrospectives et perspectives », L'évolution du droit de la protection des données : **perspectives**, in : Jusletter du 25 juin 2012
– **L'indépendance** des autorités de protection des données, pp. 71-76, in : Epiney Astrid / Hänni Julia / Brülisauer Flavia (édit.), Die Unabhängigkeit der Aufsichtsbehörden / L'indépendance des autorités de surveillance, Zurich/Bâle/Genève 2012
– Modernisation de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), 8e journée de la protection des données du 14 janvier 2014 à Vienne

WARREN ELIZABETH, Plans, How We Can Break Up Big Tech, 8 mars 2019

WARREN SAMUEL D. / BRANDEIS LOUIS D., The Right to Privacy, Harvard Law Review, 1890, pp. 193-220

WEBER ROLF H., Big Data : rechtliche Perspektive, pp. 17-36, in : Weber Rolf H. / Thouvenin Florent (édit.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zurich/Bâle/Genève 2014

WERMELINGER AMÉDÉO, Commentaire de l'art. 13 LPD, pp. 172-186, in : Baeriswyl Bruno / Pärli Kurt (édit.), Datenschutzgesetz (DSG) Stämpflis Handkommentar, Berne 2015

WERRO FRANZ / SCHMIDLIN IRÈNE, La protection de la personnalité et les médias : Une illustration de la rencontre du droit civil et du droit constitutionnel, pp. 161-217, in : Werro Franz (édit.), Droit civil et Convention européenne des droits de l'homme / Zivilrecht und Europäische Menschenrechtskonvention, Zurich/Bâle/Genève 2006

WIELE JOHANNES, Mitarbeiterdatenschutz versus Sicherheit : Das Recht hilft nur mit Diplomatie, Datenschutz und Datensicherheit 11/2009, pp. 685-689

WILDHABER ISABELLE / KASPER GABRIEL, Quantifizierte Arbeitnehmer : Empirische Daten zu People Analytics in der Schweiz, pp. 756-771, in : Festschrift für Wolfgang Portmann, Zurich/Bâle/Genève 2020

WOHLERS WOLFGANG, Commentaire de l'art. 179novies CP, pp. 542-543, in : Wohlers Wolfgang / Godenzi Gunhild / Schlegel Stefan (édit.), Schweizerisches Strafgesetzbuch, Handkommentar, 4e éd., Berne 2020

WOLFF HEINRICH AMADEUS, Commentaire de l'art. 8 Charte des droits fondamentaux, pp. 1111-1129, in : Pechstein Matthias / Nowak Carsten / Häde Ulrich (édit.), Frankfurter Kommentar EUV, GRC, AEUV, vol. 1er, Tubingue 2017

WYLER RÉMY / HEINZER BORIS, Droit du travail, 4e éd., Berne 2019

ZITTEL HEINRICH NIGGI / FUHRER STEPHAN, Datenverknüpfungen im Versicherungswesen, pp. 71-86, in : Epiney Astrid / Probst Thomas / Gammenthaler Nina (édit.), Datenverknüpfung, Problematik und rechtlicher Rahmen / L'interconnexion des données, Problématiques et cadre juridique, Zurich 2011

ZUBOFF SHOSHANA

- **Big Other** : Surveillance Capitalism and the Prospects of an Information Civilization, Journal of Information Technology 2015, pp. 75-89
- The Age of **Surveillance Capitalism**, The Fight for a Human Future at the New Frontier of Power, New York 2019

Matériaux et rapports d'organes publics ou privés

Confédération suisse

Arrêté fédéral portant approbation du protocole portant amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, FF 2020 575

Conseil fédéral
- Conséquences de la numérisation sur l'emploi et les conditions de travail : opportunité et risques, Rapport donnant suite aux postulats 15.3854 Reynard du 16 septembre 2015 et 17.3222 Derder du 17 mars 2017, 8 novembre 2017
- Modèle cible concernant le développement de formes de travail flexibles à l'administration fédérale adopté le 11 décembre 2020

Département fédéral des finances (DFF), Rapport du groupe d'experts « Avenir du traitement et de la sécurité des données » du 17 août 2018

Initiative parlementaire, Pour une réglementation destinée à instaurer de la transparence en matière de lobbyisme au Parlement fédéral
- Rapport de la Commission des institutions politiques du Conseil des États du 11 octobre 2018, FF 2018 7069
- Rapport de la Commission des institutions politiques du Conseil des États du 11 octobre 2018, Avis du Conseil fédéral, FF 2018 7659

Événements survenus au DFJP
- Rapport de la commission d'enquête parlementaire (CEP) du 22 novembre 1989, FF 1990 I 593
- Rapport complémentaire de la commission d'enquête parlementaire (CEP) du 29 mai 1990, FF 1990 II 1469

Message du Conseil fédéral à l'Assemblée fédérale concernant un projet de loi sur le travail dans l'industrie, l'artisanat et le commerce (Loi sur le travail) du 30 septembre 1960, FF 1960 II 885

Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 421

Message concernant la loi fédérale sur l'égalité entre femmes et hommes (loi sur l'égalité) et l'arrêté fédéral relatif à une modification de l'ordonnance concernant l'attribution des offices aux départements et des services à la Chancellerie fédérale du 24 février 1993, FF 1993 1163

Message relatif à l'initiative populaire fédérale « Droits égaux pour les personnes handicapées » et au projet de loi fédérale sur l'élimination des inégalités frappant les personnes handicapées du 11 décembre 2000, FF 2001 1605

Message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données du 19 février 2003, FF 2003 1915

Message concernant la loi fédérale sur l'analyse génétique humaine du 5 juillet 2017, FF 2017 5253

Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565

Office fédéral de la justice (OFJ)

- Division principale de droit public, Division projets et méthode législatifs, Modifications de l'art. 12, al. 2, let. a, LPD : Notice interprétative, janvier 2007
- Domaine de direction Droit public, Unité Projets et méthode législatifs, Loi sur la protection des données, modification du 24 mars 2006 : questions fréquentes concernant le traitement de données par des personnes privées, 30 novembre 2007
- Domaine de direction Droit public, Unité Projets et méthode législatifs, Esquisse d'acte normatif relative à la révision de la loi sur la protection des données, Rapport du groupe d'accompagnement Révision LPD du 29 octobre 2014, Référence : COO.2180.109.7.150383 / 212.9/2012/00754
- Domaine de direction Droit public, Unité Projets et méthode législatifs, Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016, Référence : COO.2180.109.7. 185665 / 212.9/2015/00001
- Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, Synthèse des résultats de la procédure de consultation du 10 août 2017
- Domaine de direction Droit public, Rapport explicatif sur la révision de l'ordonnance sur la protection des données (OPDo) du 31 août 2022
- Domaine de direction Droit public, Rapport explicatif sur la révision de l'ordonnance sur les certifications en matière de protection des données (OCPD) du 31 août 2022

Office fédéral de la statistique (OFS), Mobilité professionnelle : taux de rotation brut et net selon différentes caractéristiques, avec les changements à l'intérieur de la même entreprise, 2010-2021, tableau du 19 mai 2022

Préposé fédéral à la protection des données et à la transparence (PFPDT)
- Guide pour le traitement des données personnelles dans le secteur du travail, 2 octobre 2014
- Explications relatives aux contrôles de sécurité (employés du secteur privé), mars 2015
- Le RGPD et ses conséquences sur la Suisse, juillet 2018
- Guide relatif aux élections et votations du 6 juin 2019 (en collaboration avec les préposés cantonaux de la protection des données [privatim])
- 27e rapport d'activités 2019/2020
- 28e rapport d'activités 2020/2021
- 29e rapport d'activités 2021/2022
- Nouvelle LPD : 5 postes supplémentaires à partir de juillet 2022, 13 juillet 2021
- Rapport final et recommandations du Préposé fédéral à la protection des données et à la transparence (PFPDT) du 4 août 2021 dans le cadre de la procédure d'établissement des faits selon l'art. 29 de la Loi fédérale sur la protection des données du 19 juin 1992 concernant l'application « SocialPass » de SwissHelios Sàrl, à Oberlunkhofen et NewCom4U Sàrl, à Sierre
- Explications sur la vidéosurveillance sur le lieu de travail, publication non-datée
- Recherche, publication non-datée
- Statistique, publication non-datée

Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255

Secrétariat d'État à l'économie SECO, Commentaire de l'ordonnance 3 relative à la loi sur le travail, Art. 26 Surveillance des travailleurs, 30 mars 2016

Conseil de l'Europe

Comité consultatif pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Convention 108, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées T-PD(2017)01, 23 janvier 2017

Comité consultatif pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Convention 108, Report On Developments After The Adoption of Recommandation (2010)13 On Profiling, 26 octobre 2020

Comité des Ministres, La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, Recommandation CM/Rec(2010)13 et exposé des motifs, Strasbourg 2011

Cour EDH, Statistiques, Violation par article et par État 2020

Cour EDH, Unité de presse, Fiche thématique

- Protection des données personnelles, septembre 2022
- Surveillance au travail, janvier 2022
- Nouvelles technologies, septembre 2022

Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 10 octobre 2018

Recommandation CM/

- Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage adoptée par le Comité des Ministres du Conseil de l'Europe le 23 novembre 2010
- Rec(2015)5 sur le traitement des données à caractère personnel dans le cadre de l'emploi adoptée par le Comité des Ministres du Conseil de l'Europe le 1er avril 2015
- Rec(2018)7 sur les lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique adoptée par le Comité des Ministres du Conseil de l'Europe le 4 juillet 2018
- Rec(2021)8 du Conseil de l'Europe sur la protection des données dans le contexte du profilage adoptée par le Comité des Ministres du Conseil de l'Europe le 3 novembre 2021

Union européenne

Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, Manuel de droit européen en matière de protection des données, 2ème éd., Luxembourg 2018

Commission européenne, Livre blanc, Intelligence artificielle, Une approche européenne axée sur l'excellence et la confiance, 19 février 2020, COM(2020) 65 final

European Data Protection Supervisor (EDPS), Resolution on Privacy by Design, Jérusalem les 27 au 29 octobre 2010

Groupe de travail « Article 29 » sur la protection des données
- Avis 2/2017 sur le traitement des données sur le lieu de travail du 8 juin 2017
- Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/670 du 6 février 2018
- Lignes directrices sur le consentement au sens du règlement 2016/679 du 10 avril 2018

Nations Unies

Organisation internationale du travail
- Déclaration du centenaire de l'OIT pour l'avenir du Travail, 26 juin 2019
- Le rôle des plateformes numériques dans la transformation du monde du travail, Emploi et questions sociales dans le monde 2021, Résumé analytique

Rapporteur spécial sur le droit à la vie privée, Rapport annuel A/73/438 à l'Assemblée générale des Nations Unies du 17 octobre 2018

Organisation de coopération et de développement

Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980

OCDE, Social, Employment and Migration Working Papers
- No. 256, The Impact of Artificial Intelligence on the Labour Market : What Do We Know So Far ?, 25 janvier 2021
- No. 265, Artificial Intelligence and Employment : New Cross-Country Evidence, 15 décembre 2021

Autres institutions publiques

Commissariat à la protection de la vie privée au Canada, Les courtiers en données, Regard sur les paysages canadien et américain, Rapport préparé par le Groupe de recherche du Commissariat à la protection de la vie privée du Canada, septembre 2014

House of Commons, Digital, Culture, Media and Sport Committee, Oral Evidence : Fake News, 27 mars 2018, questions Q1388 et ss.

Organisations non-gouvernementales

AlgorithmWatch, In Catalonia the RisCanvi Algorithm Helps Decide Whether Inmates Are Paroled, 25 mai 2021

AlgorithmWatch, Automated Decisions and Artificial Intelligence in Human Resource Management, Guideline for Reviewing Essential Features of AI-Based Systems for Works Councils and Other Staff Representatives, 18 mai 2021

humanrights.ch, Lutte contre le terrorisme, Mesures policières de lutte contre le terrorisme (MPT) – L'argumentaire, 18 février 2021

Privacy International, Examples of Data Points Used in Profiling, rapport non-daté

Reatch, Wenn Künstliche [sic] Intelligenz über Bewerber*innen entscheidet, 19 octobre 2021

Reatch, Zukunft der Arbeit, Wie wirkt sich der technologische und gesellschaftliche Wandel auf unsere Arbeit aus ?, publication non-datée

Vmware, The Virtual Floorplan, New Rules for a New Era of Work, octobre 2021

World Economic Forum (WEF), Rethinking Personal Data : A New Lens for Strenghtening Trust, Prepared in Collaboration with A. T. Kearney, mai 2014

Articles de presse

ALEXANDER KATHARINA, Harvard-Professorin : « Bewerbungsgespräche sind das schlechteste Instrument, um gute Mitarbeiter*innen zu finden », EDITION F du 5 novembre 2017

BRITSKO SASCHA / SCHOOP FLORIAN / WENGER NATALIE / LEMCKE ANJA, Wer sind wir im Internet ? Wir haben den Test gemacht – mit irritierendem Ergebnis, NZZ du 13 novembre 2021

BRÜHLMANN KEVIN, Auf den Spuren des Kommunistenjägers Cincera, Der Bund du 12 août 2021

BÜTLER DANIEL, « Diese Methode ist unmenschlich », Neuer Trend : Wer einen Job will, muss sich per Video bewerben. Kann das gut gehen ?, Beobachter du 31 janvier 2017

CETOJEVIC DARCO / MESCHENMOSER MARC, Vom Bildschirm bis vor die Haustür verfolgt, K-tipp du 24 mars 2021

DIBBASEY NOA / STUDER RUEDI, « Airlines können keine Impfausweispflicht einführen », Blick du 28 décembre 2020

DI PASQUALE SYLVIA, Crystal Knows, l'IA qui publie votre test de personnalité sans vous le dire, Cadremploi du 6 juillet 2020

DUPORTAIL JUDITH, I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets, The Guardian du 26 septembre 2017

FONTI MIRJAM, Das wissen Google & Co. über Sie, K-Tipp du 13 janvier 2021, pp. 34-36

FULTERER RUTH, Warum Tracking-basierte Werbung überschätzt und auf dem Abschwung ist, NZZ du 31 mars 2021

GOLLA MATHILDE, Le logiciel de recrutement d'Amazon n'aimait pas les femmes, Le Figaro du 11 octobre 2018

GRATWOHL NATALIE, Bewerbungsgespräch am Laptop : Die Corona-Krise beschleunigt die digitale Rekrutierung, NZZ, 16 août 2020

GRATWOHL NATHALIE / RÜTTI NICOLE, Big Brother im Home-Office : Das Vertrauen der Mitarbeiter steht auf dem Spiel, NZZ du 14 décembre 2020

GROSSENBACHER TIMO, « Predictive Policing », Polizei-Software verdächtigt zwei von drei Personen falsch, SRF News du 5 avril 2018

IMBACH FLORIAN, Datenschützer : Massive Kritik am Vorschlag des Bundesrates, SRF News du 20 janvier 2016

MÄDER LUKAS / FULTERER RUTH, Plattform für Menschenhandel, Schäden bei Teenagern, falsche Nutzerzahlen : Das sind die Vorwürfe der Facebook-Whistleblowerin, NZZ du 5 octobre 2020

PASQUALE FRANK, The Other Big Brother, Government Surveillance Gets Most of Activists' Scrutiny, but Many of Today's Privacy Abuses Are Happening in the Workplace, The Atlantic du 21 septembre 2015

STECK ALBERT, Frauen werden kaum diskriminiert, wie die neue Überprüfung der Löhne zeigt, NZZ am Sonntag du 14 août 2021

THOMPSON STUART A. / WARZEL CHARLIE, Twelve Million Phones, One Dataset, Zero Privacy, The New York Times du 19 décembre 2019

TRIBELHORN MARC, Fichenaffäre von 1989 – der gefrässige Staat, NZZ du 22 novembre 2014

WASSMER PASCAL, Télétravail : la tentation de la surveillance, RTS La Matinale du 1er octobre 202

Introduction

En 1989, lorsqu'éclata le « scandale des fiches », une grande partie de la population suisse était révoltée[1]. Plusieurs manifestations eurent lieu à travers le pays. La Police fédérale et les services de renseignement cantonaux ainsi que certaines personnes privées comme p. ex. le politicien PLR zurichois ERNST CINCERA[2] avaient, pendant plusieurs dizaines d'années, édicté 900'000 dossiers secrets au sujet de personnes, d'organisations et d'événements[3] considérés représenter une « menace communiste » pour la sécurité intérieure et extérieure de la Suisse[4]. En d'autres termes, cette surveillance secrète avait pour but de protéger la Suisse contre des activités subversives communistes dans le contexte de la Guerre froide. Ces dossiers secrets connus sous le nom de « fiches » retraçaient, entre autres, des activités politiques[5] ou des voyages dans des pays de l'Europe de l'Est[6]. Toutefois, ces fiches contenaient également des observations plus anodines comme p. ex. la coutume, pour une des multiples femmes observées, de boire de la bière le soir et de vivre en concubinage[7].

À la suite de ces révélations, une Commission d'enquête parlementaire (ci-après « CEP »), présidée par le futur conseiller fédéral MORITZ LEUENBERGER, fut mise en place. Cette CEP avait pour mission d'enquêter à propos de

---

1 À la fin de son rapport, la CEP constate « que les griefs à l'encontre du Ministère public fédéral et d'autres offices du Département fédéral de justice et police ont abouti à une crise de confiance dans notre pays », voir FF 1990 I 839.

2 Pour un aperçu publié récemment des activités d'ERNST CINCERA dès les années 1970, voir BRÜHLMANN, Auf den Spuren des Kommunistenjägers Cincera.

3 On notera que « les deux tiers [des fiches] concernent des étrangers ; sur le solde, la moitié des fiches se rapporte à des personnes et l'autre moitié à des organisations ou des événements », voir FF 1990 I 776.

4 FF 1990 I 769 s.

5 FF 1990 I 777 et 788.

6 FF 1990 I 777.

7 Lorsque le scandale des fiches éclata, l'ancienne conseillère nationale thurgovienne MENGA DANUSER décida de publier sa fiche, voir, à titre d'exemple, TRIBELHORN, Fichenaffäre von 1989 – der gefrässige Staat ; pour le contenu d'une fiche d'une personne anonyme allant dans le même sens et d'autres annotations dépourvues de lien avec la sécurité intérieure ou extérieure de la Suisse, voir FF 1990 I 786 s. ; pour un aperçu des différentes fiches « dont l'existence était dans une large mesure inconnue des responsables », comme p. ex. les documents ayant trait à des employés de la Confédération indignes de confiance ou suspects, voir FF 1990 II 1487 ss.

cette surveillance secrète et d'offrir, à tout citoyen intéressé[8], la possibilité de consulter son éventuel dossier[9]. Grâce à ce travail d'enquête et à la consécration d'un droit d'accès à ces fiches, plusieurs citoyens comprirent enfin pourquoi il leur avait été impossible de trouver un emploi dans le secteur public (et parfois privé) : pour des raisons souvent obscures, ils avaient été fichés. Sur la base des informations contenues dans ces fiches – auxquelles certains employeurs avaient pu avoir accès à l'insu des candidats concernés – ces mêmes employeurs avaient décidé à ne pas engager le candidat[10].

Aujourd'hui, à titre d'exemple, tout utilisateur de l'application de rencontre *Tinder* met à disposition de cette entreprise privée américaine son nom, sa date d'anniversaire, ses différents lieux de résidence, ses photos, son numéro de téléphone, ses préférences sexuelles, son niveau de revenu, son origine ethnique, son intelligence (déterminée sur la base d'une multitude de paramètres comme p. ex. la longueur des phrases écrites ou le nombre total de mots utilisés comptant plus de trois syllabes), son état psychique (comme p. ex. son degré de nervosité) ainsi que quelques données relative à sa santé physique[11]. En bref, cette entreprise privée détient potentiellement beaucoup plus d'informations que le gouvernement suisse à propos de quelques citoyens à la fin des années 1980 et dispose, de surcroit, des connaissances techniques (intelligence artificielle)[12] afin de procéder à un traitement automatisé de ces données dans le but d'évaluer certains aspects de la personnalité des

8 Pour des raisons de lisibilité, la forme masculine est utilisée ci-après et inclut le féminin par analogie.

9 FF 1990 I 842.

10 Année politique suisse 1989, p. 23 ; BELSER, § 1, N 15 s. ; on notera l'« ironie » qu'au sortir de ses études de droit, MORITZ LEUENBERGER, alors âgé de 24 ans, ne fut pas embauché par la Direction de la santé du canton de Zurich, notamment parce qu'il figurait sur l'une des fiches de CINCERA. Ce n'est que beaucoup plus tard qu'il comprit ce refus d'embauche, voir BRÜHLMANN, Auf den Spuren des Kommunistenjägers Cincera.

11 DUPORTAIL, I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets. À la suite de la publication de cet article, DUPORTAIL a enquêté davantage sur le fonctionnement de cette application, notamment sur la mise en place d'une « note secrète de désirabilité » fondée sur le *Elo Score*. C'est dans le cadre de son enquête qu'elle est tombée sur le brevet de *Tinder* en partie repris ici, voir DUPORTAIL, pp. 21 ss. (pour le fonctionnement du *Elo Score*) et 189 ss. (pour le contenu du brevet). On notera qu'entretemps, *Tinder* aurait remplacé le *Elo Score* par une autre forme d'évaluation automatisée, voir Tinder, Powering Tinder – The Method Behind Our Matching, 11 juillet 2022.

12 « L'intelligence artificielle désigne l'intelligence de machines agissant comme des 'agents intelligents'. En tant qu'agent intelligent, certains dispositifs peuvent, avec l'aide d'un logiciel, percevoir leur environnement et agir selon des algorithmes. L'expression 'intelligence artificielle' est utilisée lorsqu'une machine imite des fonctions cognitives, telles que l'apprentissage et la résolution de problèmes, qui seraient normalement associées à des personnes physiques », voir Agence des droits fondamentaux de l'UE et Conseil de l'Europe, p. 396.

utilisateurs de cette application (profilage)[13]. Dès lors, il est facile d'imaginer que cette entreprise procède à des évaluations automatisées très détaillées de ces utilisateurs avant de revendre ces évaluations à des employeurs intéressés[14].

S'il est vrai que l'exemple *Tinder* peut sembler tiré par les cheveux et que jusqu'à ce jour, aucun scandale à propos de cette application n'a (encore) fait la une des journaux en Suisse[15], plusieurs entreprises privées, souvent basées dans un pays anglo-saxon, proposent d'effectuer un profilage de candidats dans le cadre de procédures d'embauche en Suisse. Leurs services consistent à dépouiller de nombreuses bases de données publiques[16] *et* privées puis à évaluer ces données grâce à des techniques d'intelligence artificielle afin de générer une évaluation automatisée de la personnalité des candidats. À titre d'exemple, les entreprises *HireRight* ou *Crystal Knows* proposent, voire permettent de dépouiller plusieurs bases de données à la recherche d'informations au sujet d'un candidat puis de procéder à une évaluation automatisée des données ainsi collectées dans le cadre d'une procédure d'embauche[17]. D'autres services, comme p. ex. *Outmatch Assess* (anciennement *WePow*), permettent d'automatiquement comparer un candidat avec l'un des 900 profils standardisés proposés par *HR Campus*, qui distribue ce service[18]. Plus de 1'000 entreprises suisses semblent avoir recours à une forme de profilage dans le

13 Art. 5 let. f LPD.

14 Le schéma de l'ONG *PersonalDataIO* illustre cette possibilité. Cette ONG est une association à but non-lucratif fondée par PAUL-OLIVIER DEHAYE siégeant à Genève et ayant pour but de remettre l'humain au centre des *data* en rendant les droits à la protection des données effectifs et collectivement utiles. DEHAYE est un activiste de renommée internationale. Il a notamment été au cœur de la révélation du scandale *Cambridge Analytica* et de l'enquête menée par DUPORTAIL à propos de *Tinder* ; dans le même sens, voir, pour la Suisse, FONTI, pp. 34 ss. ; dans son ouvrage publié en 2016, MORGENROTH précise qu'aux États-Unis, environ 3'600 entreprises proposent de telles évaluations. L'entreprise *First Advantage* serait un des géants du marché, voir MORGENROTH, pp. 106 ss.

15 On notera que selon DEHAYE, les données personnelles collectées puis évaluées par *Tinder* impactent les offres d'emploi visibles sur *LinkedIn* (*Your personal data affects who you see first in Tinder, yes, […] But also what job offers you have access to on LinkedIn*), voir DUPORTAIL, I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets.

16 Grâce au mouvement *Open Data*, les institutions publiques mettent davantage de données personnelles à disposition, le plus souvent gratuitement. Ainsi, les entreprises privées intéressées disposent de sources de données supplémentaires. Cette réalité leur permet d'affiner encore plus leurs évaluations automatisées, voir BERANEK ZANON, p. 89 ; dans une veine similaire mettant en garde contre l'utilisation, par des privés, de données personnelles accessibles au public, voir ZUBOFF, Surveillance Capitalism, pp. 272 s.

17 PFPDT, 28e rapport d'activités, p. 47 ; DI PASQUALE, Crystal Knows, L'IA qui publie votre test de personnalité sans vous le dire.

18 Le site de HR Campus n'est disponible qu'en allemand ou en anglais, ce qui laisse penser que l'entreprise ne s'est pas (encore) établie en Suisse romande, voire en France voisine.

cadre de procédures d'embauche comme p. ex. les CFF, le supermarché Migros ainsi que plusieurs banques cantonales[19]. Cette tendance s'est accentuée dans le cadre de la pandémie de Covid-19[20].

Si le cadre légal de la pratique de ficher les citoyens a été étudié en profondeur par la CEP compétente[21], le cadre légal qui gouverne le recours à la pratique du profilage dans le cadre d'une procédure d'embauche soumise au droit privé – forme de surveillance privée – quant à lui reste à être analysé, voire complété. En effet, au vu de l'exemple cité en guise d'introduction, différentes questions juridiques se posent.

A. Questions de droit

L'exemple esquissé est une illustration possible du fait qu'un profilage effectué dans le cadre d'une procédure d'embauche peut non seulement porter atteinte à la personnalité de la personne candidate, mais aussi à certains intérêts protégés par les droits fondamentaux de celle-ci.

Ainsi, on peut d'abord se demander si, dans le cadre d'une procédure d'embauche, un employeur établi en Suisse peut procéder à un traitement automatisé des données personnelles de la personne candidate, notamment dans le but d'évaluer certains éléments de sa personnalité concernant son futur rendement au travail (profilage). En d'autres termes, est-ce que le recours à cette forme de traitement de données dans le contexte d'une procédure d'embauche est légal en vertu du droit suisse ?

Si un tel traitement de données personnelles est en principe licite, il convient, dans un deuxième temps, de déterminer les éventuelles limites à ce traitement de données personnelles.

---

19 Plus de 1'000 entreprises suisses-alémaniques semblent faire recours à l'un des services proposés par *HR Campus*, voir HR Campus, Referenzen, Kunden, die HR Campus vertrauen. Étant donné que plusieurs entreprises offrent de tels services sur le marché suisse, le nombre des employeurs procédant à une forme de profilage au stade de la procédure d'embauche doit être considérablement plus haut.

20 GRATWOHL, Bewerbungsgespräch am Laptop : die Corona-Krise beschleunigt die digitale Rekrutierung.

21 FF 1990 I 769 ss., pour les propositions mises en avant par la CEP après l'analyse du cadre légal jugé insuffisant, voir FF 1990 I 801 ss. ; cette constatation ne devrait toutefois pas conduire à la conclusion que les nouvelles mesures mises en place par les services de renseignement suisses ne suscitent plus de questions. Ainsi, CUPA a dédié sa thèse soutenue en 2014 à l'Université de Zurich aux garanties procédurales en cas de surveillance étatique préventive. Dans son introduction, il relève qu'il n'existe que peu de publications juridiques à ce sujet en Suisse, voir CUPA, N 11 ; dans une veine plus politique, on pensera, à titre d'exemple, aux débats qui ont entouré la votation sur la nouvelle Loi fédérale du 25 septembre 2020 sur les mesures policières de lutte contre le terrorisme (MPT), voir, à titre d'exemple, humanrights.ch, Lutte contre le terrorisme, Mesures policières de lutte contre le terrorisme (MPT) – L'argumentaire du 18 janvier 2021.

Dans un troisième et dernier temps on peut se demander si ce cadre légal s'avère en effet apte à éviter des atteintes au droit de la personnalité des personnes candidates et à leurs intérêts protégés par leurs droits fondamentaux. Si le cadre légal défini s'avérait inefficace à garantir le respect des droits des candidats, quelles mesures d'ordre juridique pourraient être mises en œuvre afin de garantir une meilleure protection de ces droits ?

Une analyse de ces différentes questions s'avère nécessaire non seulement lorsqu'il s'agit d'apporter une réponse juridique à l'exemple cité en guise d'introduction, mais aussi d'une manière plus générale – et ceci pour plusieurs raisons.

B. Intérêts de la contribution

D'abord, il convient de noter que la collecte de données personnelles puis l'analyse automatisée desdites données dans le but d'évaluer certains aspects de la personnalité d'un individu ou d'un groupe de personnes deviennent de plus en plus précises et de moins en moins coûteuses[22]. Les chiffres récents montrent que le secteur économique des *data broker*[23] est en pleine expansion ce qui se traduit, entre autres, par une augmentation d'employeurs suisses ayant recours à ce genre de services[24]. Il est donc fort probable que le recours à ces traitements de données pendant la procédure d'embauche deviendra encore plus fréquent dans les années à venir[25]. Ces développements récents ont également influencé le Parlement suisse, qui a adopté une définition légale du profilage en 2020 et qui a décidé de mentionner, à titre d'exemple, la relation de travail en tant que première relation juridique potentiellement affectée par

22 WALTER, Le profilage, p. 87.

23 La notion de « data broker » (anglais pour « courtier en données ») fait référence aux entreprises qui collectent des données, y compris des données personnelles de consommateurs, en provenance d'une multitude de banques de données différentes dans le but de revendre ces données à leurs clients, qui sont des entreprises privées ou des agences gouvernementales, voir CHRISTL/SPIEKERMANN, p. 87. En français, la notion de « courtier en données » est parfois utilisée. Toutefois, étant donné que cette expression est plutôt rare dans la littérature spécialisée, la notion anglaise, beaucoup plus courante, sera utilisée dans cette contribution ; voir également REINSCH/GOLTZ, p. 37 ; pour un aperçu critique à propos de ce secteur économique naissant, publié à la fin des années 1990, voir SCHWEIZER A., pp. 97 ss. ; pour un reportage de deux journalistes suisses, qui relatent, entre autres, les pratiques peu transparentes des *data broker* suisses *Künzler-Bachmann* et *Intrum*, voir BRITSKO/SCHOOP/WENGER/LEMCKE, Wer sind wir im Internet ? Wir haben den Test gemacht – mit irritierendem Ergebnis.

24 Pour une appréciation abstraite et plutôt générale de cette tendance en Suisse, voir KASPER/WILDHABER, Big Data am Arbeitsplatz, p. 192 et PFPDT, 28e rapport d'activités, p. 47 ; pour une analyse empirique de cette tendance en Suisse, voir WILDHABER/KASPER, Quantifizierte Arbeitnehmer, pp. 760 et ss.

25 WILDHABER/KASPER, Quantifizierte Arbeitnehmer, pp. 770 s.

cette nouvelle forme de traitement de données[26]. Cette évolution s'est aussi fait ressentir dans le cadre de mon activité professionnelle. En effet, en tant que collaboratrice scientifique auprès du Préposé fédéral à la protection des données et à la transparence[27] (ci-après « PFPDT »), j'ai été consultée à de nombreuses reprises soit par des employeurs qui comptaient soumettre certains candidats à un profilage soit par des candidats « profilés » qui souhaitaient se renseigner sur les moyens juridiques leur permettant de s'opposer à ce traitement de données[28]. Au vu des développements récents, il est donc nécessaire d'analyser le nouveau cadre légal et de proposer quelques réponses possibles aux questions auxquelles la (nouvelle) LPD de septembre 2020 n'apporte (potentiellement) pas de réponse (satisfaisante).

Ensuite, l'analyse qui suit a pour but d'ouvrir des pistes de réflexion afin de mieux cerner une nouvelle problématique qui a le potentiel d'affecter une majorité de la population suisse. En effet, la majorité des personnes en âge de travailler ont qualité d'employé et non d'employeur ou d'indépendant. De plus, les statistiques officielles montrent que chaque année, le nombre d'employés qui changent d'emploi augmente[29]. Ainsi, la probabilité qu'un plus grand nombre de personnes doivent se soumettre un jour à un profilage dans le cadre d'une procédure d'embauche ne devrait pas être sous-estimée.

Par ailleurs, cette contribution s'inscrit dans le cadre d'un mouvement plus large qui vise à étudier l'impact des nouvelles formes de traitements de données sur le monde du travail. Elle visera donc à proposer une réponse possible à une question (parmi beaucoup d'autres) qui se pose dans ce domaine et qui n'a pas encore reçu de réponse à ce stade en Suisse[30]. En effet, trois grandes thématiques ont été abordées par la doctrine suisse quant à l'impact de ces nouveaux traitements de données sur le monde du travail : savoir quelles places de travail vont, dans un avenir proche, disparaître et quelles places, au contraire, vont être créées, ensuite, savoir quelles nouvelles conditions de travail vont être imposées aux employés[31] et, enfin, savoir quelles nouvelles formes de travail

26 Art. 5 let. f LPD.

27 Art. 49 ss. LPD.

28 PFPDT, 28e rapport d'activités, p. 47.

29 Office fédéral de la statistique (OFS), Mobilité professionnelle : taux de rotation brut et net selon différentes caractéristiques, avec les changements à l'intérieur de la même entreprise, 2010-2021, tableau du 19.05.2022. On relèvera la légère baisse des deux taux de rotation en 2020 et 2021, qui est très probablement due à la pandémie du Covid-19.

30 Dans un sens plus général à propos des nouveaux traitements de données, voir HEUBERGER, N 12.

31 Dans le cadre de la pandémie du Covid-19, ces questions sont devenues encore plus pressantes avec l'avènement presque généralisé du télétravail, voir, pour le secteur privé, PFPDT, 28e rapport d'activités, p. 48 ; pour le secteur public fédéral, voir Conseil

vont caractériser le marché du travail de demain. Cependant, se demander quel impact les traitements de données de plus en plus intrusifs pourraient avoir sur la relation précontractuelle qui lie l'employeur et la personne candidate n'est que très peu, voire pas du tout abordée par la doctrine[32]. Ainsi, cette contribution s'inscrit dans la continuité d'un projet de recherche novateur soutenu par le Fonds national suisse à la recherche[33] et d'une thèse publiée en 2020 à l'Université de Lucerne[34]. En d'autres termes, cette contribution a pour but de contribuer à la discussion commencée il y a quelques années au sujet de l'impact du *Big Data*[35] sur la relation de travail.

En outre, la plupart des questions juridiques soulevées lorsqu'il est fait recours au profilage doivent être analysées au cas par cas dans la mesure où les traitements de données sont avant tout régis par des principes généraux[36]. En d'autres termes, une réponse contraignante à la plupart des questions définies plus haut ne pourra qu'être donnée dans le cadre d'un litige[37]. Ainsi, j'ai l'espoir que cette contribution puisse offrir une piste de réflexion aux juges qui seraient amenés à trancher l'une des multiples questions liées au profilage dans le cadre d'une procédure d'embauche, p. ex. après l'ouverte d'une enquête engagée par le PFPDT en tant qu'autorité de surveillance[38].

fédéral, Modèle cible concernant le développement de formes de travail flexibles à l'administration fédérale adopté le 11 décembre 2020.

32 KAUFMANN/SCHUERCH, Positionspapier, p. 3 ; dans le même sens, voir DUNAND/MAHON/WITZIG, p. 4 ; cette lacune ne semble pourtant pas être une spécificité suisse, voir GUTWIRTH/HILDEBRANDT, p. 34. LEMPEN, quant à elle, relève avant tout une nécessité de réflexions plus approfondies quant à l'articulation entre les différentes dispositions légales applicables dans le cadre d'une procédure d'embauche, voir LEMPEN, p. 270.

33 Fonds national suisse de la recherche scientifique, Big Data or Big Brother ? – Big Data HR Control Practices and Employee Trust, n° 167209, WILDHABER ISABELLE et al., 1.3.2017-28.2.2021.

34 HEUBERGER, N 1 ss.

35 Le terme « *Big Data* » (ou, parfois, francisé « mégadonnées ») est une expression à la mode qui peut désigner plusieurs concepts en fonction du contexte. Selon l'Agence des droits fondamentaux de l'UE et Conseil de l'Europe, cette notion « recouvre généralement 'la capacité technologique croissante de collecter, traiter et extraire très rapidement des connaissances nouvelles et prédictives à partir d'un gros volume et d'une grande variété de données' », voir Agence des droits fondamentaux de l'UE et Conseil de l'Europe, p. 395 ; PROBST a qualifié les défis posés par les nouveaux traitements de données permettant des appariements de données inconcevables avant l'avènement du *Big Data* de « [traduction] problème fondamental de nos sociétés modernes interconnectées », voir PROBST, p. 39 ; dans le même sens, voir MEIER, Protection des données, N 299 s.

36 KASPER/WILDHABER, Big Data am Arbeitsplatz, p. 227 ; pour une constatation similaire en droit du Conseil de l'Europe, voir MARSCH, p. 8.

37 ROSENTHAL, Das neue Datenschutzgesetz, N 25.

38 Art. 49 ss. LPD (art. 29 aLPD).

De surcroît, même avant l'avènement du *Big Data*, les responsables des ressources humaines devaient trouver un équilibre entre l'intégrité personnelle des employés d'une part (leur capacité à agir selon leurs propres valeurs en toutes circonstances) et le devoir de loyauté qui incombe aux employés d'autre part (leur devoir de se conformer, en toutes circonstances, aux exigences et aux valeurs de leur employeur)[39]. Cette tension a été thématisée par le Conseil fédéral en 1988 déjà lorsqu'il écrivait à propos de la nouvelle Loi sur la protection des données : « L'objectivité des décisions relatives au personnel, de même que la protection de la personnalité des employés ont tout à gagner de la rationalisation de la gestion du personnel au moyen des méthodes modernes de traitement des données ; ces méthodes sophistiquées n'ont cependant pas que des effets positifs : elles sont de nature à révéler presque toutes les facettes de la personnalité d'un employé, transparence que ne justifient en aucun cas les besoins réels de l'entreprise »[40]. Les publications d'auteurs qui ont eu l'occasion d'analyser quelques conséquences des nouveaux traitements de données dans le monde du travail laissent penser que les réserves émises par le Conseil fédéral il y a plus de 30 ans étaient justifiées et que le déséquilibre mentionné par le Conseil fédéral risque de s'accentuer davantage dans les années à venir[41]. Ainsi, il est indiqué de réfléchir à un cadre légal qui pourrait améliorer l'équilibre entre ces deux besoins contradictoires.

Enfin, le profilage n'est pas uniquement utilisé dans le cadre d'une procédure d'embauche. En effet, ce nouveau traitement de données peut être effectué dans des contextes très divers, p. ex. lorsqu'il s'agit d'octroyer ou non un crédit[42], de déterminer la hauteur d'une prime d'assurance[43], de décider de la liberté conditionnelle ou non d'un détenu[44] ou de choisir le client qui mérite

39 LEICHT-DEOBALD et al., pp. 382 s.

40 FF 1988 II 494 ; dans sa thèse qui portait sur la procédure d'embauche et la protection des données (*Stellenbewerbung und Datenschutz*), publiée peu après l'entrée en vigueur de l'aLPD, RUDOLPH semble confirmer la position du Conseil fédéral, voir RUDOLPH, Stellenbewerbung und Datenschutz, pp. 136 ss.

41 Ainsi, LEICHT-DEOBALD et al. précisent que cette tendance est due à trois facteurs : une diminution des opportunités pour les personnes concernées de comprendre les décisions automatisées prises à leur égard, la tendance à se fonder sur des mesures techniques dans des contextes où une certaine réflexion (humaine) serait de mise et un manque d'imagination morale pour affronter certaines décisions qui doivent être prises par les responsables RH, voir LEICHT-DEOBALD et al., p. 383 ; PASQUALE, The Other Big Brother.

42 Dans le contexte du crédit, la notion de « credit scoring » est souvent employée. À titre d'exemple, voir O'NEIL, pp. 141 ss. ; PASQUALE, Black Box Society, pp. 41, 56 et 114 ; MORGENROTH, pp. 31 ss.

43 À titre d'exemple, voir O'NEIL, pp. 161 ss.; THOUVENIN, Individualisierung, p. 16.

44 À titre d'exemple, voir O'NEIL, pp. 24 ss.

d'être servi en premier dans un *call center*[45]. J'ai l'espoir que la réflexion qui suit puisse servir de source d'inspiration à la réglementation d'autres relations juridiques non moins sensibles que celle qui lie le candidat à son futur employeur faisant face, elles aussi, aux défis liés à l'utilisation du profilage[46].

Les intérêts de la contribution ainsi esquissés, il convient de circonscrire la méthode choisie afin d'apporter des réponses aussi nuancées que possibles aux questions définies plus haut.

C. Méthodologie

La présente contribution répondra aux questions définies d'un point de vue d'un candidat « profilé » établi en Suisse. Ainsi, l'analyse qui suit portera sur les lois fédérales suisses potentiellement applicables à un profilage effectué lors d'une procédure d'embauche.

S'il est certain que la Suisse n'est pas un État membre de l'Union européenne (ci-après « UE ») et que le droit européen n'est, en principe, pas applicable en Suisse, la jurisprudence de la Cour de justice de l'UE (ci-après « CJUE ») est une source d'inspiration importante en droit suisse. Dans quelques domaines restreints, la jurisprudence de cette cour doit impérativement être respectée par le Tribunal fédéral[47] ; dans d'autres domaines, le Tribunal fédéral interprète le droit suisse conformément au droit européen, souvent lorsque le Législateur a rendu la loi litigieuse « eurocompatible » en amont[48],

45 En 2009 déjà, plusieurs entreprises suisses, dont l'*UBS*, *Helsana* et la *Bâloise assurance*, évaluaient leurs clients sur la base de différents critères et répartissaient leurs clients dans des catégories distinctes. Grâce à un logiciel intelligent, ces entreprises pouvaient isoler les clients particulièrement intéressants, notamment d'un point de vue lucratif. Ce profilage permettait au centre d'appel de reconnaître la valeur des clients qui appelaient afin de privilégier les bons clients et de faire patienter les autres, voir WALTER, Le profilage, p. 89.

46 Groupe de travail « Article 29 » sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, pp. 5 s. ; Privacy International, Examples of Data Points Used in Profiling, pp. 26 ss. ; pour davantage d'exemples d'utilisations problématiques de différentes formes de profilage qui risquent avant tout d'impacter les personnes issues de milieux modestes aux États-Unis, voir EUBANKS, pp. 39 ss.

47 À titre d'exemple, voir l'art. 1er Protocole 2 concernant l'interprétation uniforme de la convention de Lugano, tel que mentionné par NIANG, pp. 193 s.

48 À titre d'exemple, l'art. 4 al. 5 aLPD (règle aujourd'hui consacrée à l'art. 6 al. 6 et 7 LPD), a été introduit dans l'aLPD afin de rendre l'aLPD plus compatible avec le droit européen. Dans ce contexte, l'OFJ avait déclaré en 2006 déjà que « la révision rapproche le droit suisse de la directive européenne sur plusieurs points. L'interprétation de la directive par les autorités étrangères de protection des données ou par le groupe visé à l'art. 29 de ce texte peut, sur ces points, donner des indications quant à leur application pratique. S'il s'agit de concrétiser un des principes matériels en matière de protection des

parfois même en l'absence d'une telle volonté législative[49]. Dans ce contexte, on rappellera qu'en matière du droit de la protection des données, la CJUE est l'autorité judiciaire la plus influente en Europe (et au-delà)[50].

L'UE a joué un rôle précurseur dans l'encadrement du profilage en adoptant le Règlement général sur la protection des données[51] (ci-après « RGPD ») en 2016. En effet, le RGPD, entré en vigueur en mai 2018, est le premier dispositif légal de nature contraignante qui vient définir et encadrer le traitement de données connu sous le nom de « profilage »[52]. Un des buts de la révision de l'ancienne loi fédérale sur la protection des données du 19 juin 1992 (ci-après « aLPD ») était précisément de s'inspirer du travail pionnier de l'UE et de rendre le droit suisse « eurocompatible » en amont (sans pour autant procéder à un copier-coller[53]). En effet, le Législateur suisse souhaitait, entre autres, mettre en place un cadre légal qui permette aux entreprises suisses de continuer à facilement échanger des données personnelles avec des entreprises établies dans l'UE[54]. Ainsi, la définition européenne du « profilage » a été reprise en droit suisse[55].

données, on peut en général considérer qu'une pratique conforme à la directive satisfera aux exigences de la LPD », voir Office fédéral de la justice (OFJ), Loi sur la protection des données, modification du 24 mars 2006 : questions fréquentes concernant le traitement de données par des personnes privées, 30 novembre 2007, p. 1 ; pour une analyse plus approfondie de cette influence européenne en matière de consentement, voir VASELLA, Einwilligung, N 30 ss.

49 BESSON cite, à titre d'exemple, les ATF 137 III 487 et ATF 137 II 199, voir BESSON, Droit constitutionnel européen, N 1386.

50 FABBRINI, p. 22.

51 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit Règlement général sur la protection des données.

52 Groupe de travail « Article 29 » sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, p. 6.

53 ROSENTHAL, Das neue Datenschutzgesetz, N 10.

54 Dans les domaines qui ne relèvent pas de la coopération instaurée par Schengen et Dublin, la Suisse est considérée comme un État tiers. Or, l'échange de données entre un État tiers, c'est-à-dire la Suisse, et les États membres ne peut qu'avoir lieu si la Suisse assure un niveau de protection des données adéquat au sens du droit européen pertinent. Depuis l'arrêt de la CJUE rendu dans l'affaire *Schrems I* du 6 octobre 2015, l'UE est tenue de procéder à un suivi périodique du niveau de protection adéquat des données assuré par les États tiers, dont la Suisse. Ainsi, si la Suisse entend obtenir à nouveau une telle décision d'adéquation, il est essentiel qu'elle adapte sa législation au cadre européen, voir, pour les détails, FF 2017 6588 et, pour une analyse approfondie des critères qui risquent d'être déterminants, voire problématiques lors de l'examen du régime suisse, voir MÖHLE, pp. 599 ss.

55 FF 2017 6641.

Il convient de noter que le RGPD a pour but de protéger les personnes qui se trouvent sur le territoire de l'EEE[56], indépendamment du lieu de résidence du responsable du traitement. Cette protection ainsi conçue peut impliquer une application extraterritoriale du RGPD[57]. Dans le cadre de cette contribution, force est de constater que malgré son application extraterritoriale dans certaines hypothèses[58] (que la jurisprudence viendra sans doute préciser[59]), le RGPD ne s'appliquera pas aux traitements de données effectués par un employeur suisse qui recrute un candidat qui se trouve dans l'espace EEE au moment de la candidature[60]. En d'autres termes, le RGPD ne s'applique pas directement aux procédures de recrutement menées en Suisse[61]. Étant donné que le Législateur suisse a repris la notion européenne de « profilage », le droit européen sera analysé afin de s'en servir en tant que source d'inspiration (uniquement), notamment lorsqu'il s'agira d'interpréter le nouveau droit suisse[62].

Ensuite, il convient de relever que traditionnellement, le droit de la protection des données applicable entre personnes privées était conçu comme l'une des multiples concrétisations du droit de la personnalité tel que protégé par le

56 Le 6 juillet 2018 le Comité mixte a décidé d'intégrer le RGPD dans l'Accord EEE. En d'autres termes, le RGPD s'applique également en Norvège, au Liechtenstein et en Islande, pour une analyse critique de cette décision, voir MÉTILLE/ACKERMANN, p. 79.

57 MÉTILLE/ACKERMANN, p. 81.

58 Art. 3 RGPD.

59 Pour les difficultés pratiques liées à la mise en œuvre extraterritoriale du RGPD, voir MÉTILLE/ACKERMANN, pp. 81 ss. ; en guise de rappel, il convient de noter que le PFPDT n'est pas compétent pour interpréter la portée extraterritoriale exacte du RGPD. Toutefois, il a publié, sur son site web, quelques indications quant à l'application possible du RGPD en Suisse, voir PFPDT, Le RGPD et ses conséquences sur la Suisse, Guide de juillet 2018.

60 Le RGPD s'applique dans les hypothèses où le responsable du traitement est établi en dehors de l'EEE et offre explicitement des biens ou des services à des personnes qui sont sur le territoire de l'EEE ou vise le suivi du comportement sur Internet de personnes présentes sur le territoire de l'EEE. Proposer un emploi à un ressortissant européen n'équivaut pas à fournir un service sur le territoire de l'EEE au sens de l'art. 3 al. 2 let. a RGPD, pour une analyse plus détaillée, voir MÉTILLE/ACKERMANN, pp. 82 ss. ; pour un avis contraire, voir DAEDELOW, pp. 34 ss.

61 Si le RGPD ne s'appliquera pas directement au cas d'espèce, on rappellera qu'un certain nombre d'entreprises suisses sont soumises, pour certains traitements envisagés, et au RGPD et à la LPD et ont fait le choix, pour *tous* les traitements de données effectués, de ne respecter uniquement que les exigences découlant du RGPD estimant que ce dispositif offrait une protection plus complète, voir ROSENTHAL, Entwurf, N 138.

62 Dans le même sens, voir ROSENTHAL, Das neue Datenschutzgesetz, N 10 s. ; pour une suggestion allant dans le même sens sous le régime de l'aLPD, voir Office fédéral de la justice (OFJ), Loi sur la protection des données, modification du 24 mars 2006 : questions fréquentes concernant le traitement de données par des personnes privées, 30 novembre 2007, p. 1.

Code civil[63] (ci-après « CC »). Au contraire, le droit de la protection des données applicable aux organes fédéraux avait non seulement pour but de protéger la personnalité des citoyens, mais constituait aussi une des multiples concrétisations de divers droits fondamentaux[64]. Cette conception du droit de la protection des données applicable entre particuliers n'a pas été modifiée dans le cadre de la révision de la LPD. Toutefois, cette conception diffère de celle adoptée en droit européen avec l'entrée en vigueur du RGPD. En effet, en adoptant le RGPD, l'UE a implanté une nouvelle approche selon laquelle entre particuliers (aussi) le droit de la protection des données vient non seulement protéger la personnalité des personnes concernées, mais aussi protéger leurs droits fondamentaux[65].

En raison de l'influence du droit européen sur l'ordre juridique suisse, il convient d'analyser les questions définies non seulement à la lumière de la LPD (et des autres dispositions fédérales applicables), mais également à la lumière des droits fondamentaux consacrés dans la Constitution suisse. Analyser si l'État a honoré ses obligations positives en la matière s'impose d'autant plus que « les progrès technologiques [...] mènent à un traitement de données massif et sans frontières. L'État ne représente plus la seule menace : un tel traitement est régulièrement le fait d'acteurs privés »[66].

Au vu de la portée de la CEDH dans l'ordre juridique suisse[67] et de l'impact de la jurisprudence de la Cour EDH à travers l'Europe en matière de protection des données[68], une analyse du cadre constitutionnel suisse serait incomplet

63 Code civil suisse du 10 décembre 1907, RS 210. Cette approche est également reflétée par le fait que les actions mises à disposition des personnes concernées sont les mêmes que celles qui sont prévues par le CC. En effet, l'art. 32 al. 2 LPD renvoie expressément aux actions concernant la protection de la personnalité prévues aux art. 28, 28*a* et 28*g* à 28*l* du CC.

64 ROSENTHAL, Das neue Datenschutzgesetz, N 12 ; MÉTILLE, La (nouvelle) loi fédérale, p. 6.

65 Art. 1er al. 2 RGPD ; voir, pour plus de précisions quant à cette différence de régime, ROSENTHAL, Entwurf, N 15.

66 HERTIG RANDALL/MARQUIS, art. 13 Cst., N 63 ; plus critique encore par rapport aux traitements de données effectués par des acteurs privés, MARSCH affirme que « [traduction] les entreprises privées traitent aujourd'hui des données personnelles à une échelle qui dépasse probablement de loin les traitements de données effectués par les organes publics », voir MARSCH, p. 247.

67 On rappellera qu'en raison de l'approche moniste qui prévaut en Suisse, « le Tribunal fédéral considère les droits de la CEDH comme des droits constitutionnels à part entière au sens de l'art. 189 al. 1er let. a Cst. Rien n'empêche donc [...] une application horizontale en droit privé au même titre que le droit constitutionnel national », voir BESSON, Humaniser le droit privé, p. 9 ; MALINVERNI, HOTTELIER, HERTIG RANDALL et FLÜCKIGER précisent que « la CEDH occupe une place privilégiée parmi les conventions relatives aux droits humains ratifiées par la Suisse », voir, pour les raisons d'une telle qualification, MALINVERNI/HOTTELIER/HERTIG RANDALL/FLÜCKIGER, N 2395 ss.

68 Pour l'impact de cette jurisprudence sur la Suisse, voir EPINEY/SCHLEISS, § 3, N 8 ; pour l'impact de cette jurisprudence sur l'UE et, plus spécifiquement sur le développement de l'art. 8 Charte, voir MARSCH, pp. 7 ss.

sans inclure une analyse de la jurisprudence pertinente de la Cour de Strasbourg. Dès lors, la présente contribution se penchera également sur les développements jurisprudentiels de la Cour EDH.

Plusieurs contributions ont déjà pu montrer que les défis imposés par les nouvelles formes de traitements de données ne pourront être relevés uniquement si certains facteurs économiques, technologiques, psychologiques *et* légaux sont pris en compte[69]. Consciente que la thématique définie touche aux sciences juridiques, à la psychologie[70], à la gestion d'entreprise[71], aux statistiques[72] et à l'informatique[73], la contribution abordera ladite thématique d'un point de vue juridique avant tout. Ce choix se justifie pour des raisons de brièveté et des raisons évidentes liées à ma formation. Néanmoins, certaines analyses relevant des autres disciplines mentionnées seront citées afin de compléter, voire nuancer l'argument juridique. Il va sans dire qu'une analyse complète de la thématique implique une approche interdisciplinaire.

En bref, la thématique choisie sera abordée d'un point de vue suisse (principalement) et européen (subsidiairement). Au vu de la nouvelle approche au droit de la protection des données entre particuliers, adoptée par l'UE, et des risques pour certains intérêts protégés par les droits fondamentaux des candidats soumis au profilage, l'analyse inclura une réflexion sur la portée possible des garanties constitutionnelles face à ce nouveau traitement de données. Une telle réflexion serait incomplète si elle n'incluait pas la jurisprudence de la Cour EDH, qui a eu un impact considérable en matière de protection des données. S'il est certain que la thématique soulève de nombreuses questions qui ne relèvent pas (directement) des sciences juridiques, la présente contribution a pour but d'apporter une réponse de nature juridique aux questions définies. Après avoir décrit ce que cette contribution tente d'offrir, il convient de préciser ce que cette contribution ne saurait offrir.

Les plus grandes entreprises dans le domaine du profilage sont basées aux États-Unis et donc, le plus souvent, soumises au droit fédéral américain (et aux

69 GASSER, pp. 374 s.; ZUBOF, Big Other, pp. 75 ss.; Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Report on Developments after the Adoption of Recommendation (2010)13 on Profiling, p. 5.

70 À titre d'exemple, KOSINSKI et al., pp. 493 ss. Ses travaux de recherche ont été utilisés, entre autres, par l'entreprise britannique *Cambridge Analytica* afin d'influencer les élections américaines en 2016, voir, pour plus de détails, CHRISTL/SPIEKERMANN, pp. 26 s.; HEUBERGER, quant à lui, se fonde sur les stéréotypes tels qu'entendus en psychologie sociale afin d'expliquer la notion de profilage, voir HEUBERGER, N 61.

71 KASPER/WILDHABER, Big Data am Arbeitsplatz, p. 191.

72 HELFRICH, art. 4 RGPD, N 87.

73 HILDEBRANDT, p. 17.

droits étatiques respectifs)[74]. Ainsi, on peut se demander s'il serait intéressant de comparer le cadre légal suisse à celui qui est actuellement en vigueur aux États-Unis.

Étant donné que les États-Unis n'ont pas consacré une garantie de la sphère privée dans leur Constitution fédérale[75], que la protection des données est en grande partie consacrée au niveau des États et non au niveau fédéral[76] et que ce pays fait partie des pays de tradition du *Common Law,* une comparaison entre la législation suisse d'une part et américaine d'autre part s'avérerait très compliquée et que peu utile d'un point de vue strictement pratique. Il ne fait aucun doute que d'un point de vue sociologique, une meilleure compréhension du cadre légal américain pourrait s'avérer intéressante dans la mesure où elle permettrait de mieux comprendre l'approche avec laquelle les entreprises susmentionnées offrent leurs services sur le marché suisse et/ou européen. Pour des raisons de brièveté toutefois, une analyse du cadre légal américain ne fera pas l'objet de cette contribution.

Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du Conseil de l'Organisation de coopération et de développement économiques[77] (ci-après « OCDE ») ainsi que le Pacte II de l'Organisation des Nations Unies[78] (ci-après « ONU ») ne seront pas analysés plus en détails dans cette contribution. S'agissant de dispositions qui ne confèrent pas de droits individuels directement justiciables, ces documents serviront uniquement de source d'inspiration lorsqu'il s'agira d'affiner le raisonnement juridique. Dans la même veine, il ne sera uniquement fait référence aux publications du Rapporteur spécial des Nations Unies sur le droit à la sphère

74 CHRISTL/SPIEKERMANN, p. 94.

75 KOKOTT/SOBOTTA, p. 223 ; La Déclaration des droits, qui comprend les 10 premiers amendements à la Constitution américaine, protège quelques aspects relevant du droit au respect de la sphère privée. Il est controversé de savoir si ces différentes dispositions consacrent un véritable droit au respect de la vie privée tel qu'il est prévu dans de nombreuses constitutions européennes et plusieurs traités, voir, y compris pour une analyse quant aux raisons pour lesquelles même le 4e amendement n'offrirait pas une protection de la sphère privée, SOLOVE, pp. 93 ss., mais surtout pp. 100 s.

76 REHM, Judicial Activism, p. 51 ; pour un aperçu de la « mosaïque complexe d'exigences en matière de protection de la vie privée et de sécurité des données » tant au niveau fédéral qu'étatique, voir Commissariat à la protection de la vie privée au Canada, pp. 2 s.

77 Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980.

78 Pacte international relatif aux droits civils et politiques du 16 décembre 1966, RS 0.103.2, entré en vigueur en Suisse le 18 septembre 1992, qui vient concrétiser une partie des droits consacrés dans la DUDH du 10 décembre 1948.

privée[79] où il en sera jugé nécessaire. Il en va de même avec celles du Conseil sur l'intelligence artificielle de l'OCDE[80].

L'exemple introductif laisse deviner qu'en fonction des données traitées, l'employeur peut potentiellement porter atteinte à plusieurs intérêts protégés par les droits fondamentaux du candidat, comme p. ex. au droit à l'autodétermination en matière informationnelle, au droit au respect de la sphère privée, à l'interdiction de discrimination, au droit d'être entendu, à la liberté de religion ou d'expression ; une restriction trop importante de l'usage des nouveaux traitements de données risque de porter atteinte à la liberté économique de l'employeur. Contrairement à l'interdiction de discrimination ou au droit fondamental au respect de la sphère privée, la portée du droit fondamental à l'autodétermination en matière informationnelle face aux nouveaux traitements de données, n'a pas (encore) été étudiée dans de nombreuses publications. Les quelques publications à ce sujet proposent des approches divergentes[81]. Ce constat est d'autant plus étonnant que contrairement aux deux autres droits fondamentaux mentionnés, le droit fondamental consacré à l'art. 13 al. 2 Cst., aurait le potentiel de « [traduction] rééquilibrer l'asymétrie de pouvoir et d'information entre les individus et les personnes physiques ou morales qui collectent, sauvegardent et évaluent les données »[82] et se caractérise par un plus grand champ d'application matériel dans la mesure où il couvre tous les traitements de données personnelles (et non uniquement les

79 Le rapporteur spécial est un expert indépendant chargé par le Conseil des droits de l'homme d'étudier la situation d'un pays ou un thème spécifique relevant des droits de l'homme, et d'en rendre compte. Il s'agit d'un poste à titre honorifique : l'expert ne fait pas partie du personnel des Nations Unies et n'est pas rémunéré pour son travail. À la suite des révélations d'EDWARD SNOWDEN, le Conseil des droits de l'homme a nommé le premier Rapporteur spécial sur le droit à la vie privée en juillet 2015, voir Nations Unies, Droits de l'homme, Haut-Commissariat, Rapporteur spécial sur le droit à la vie privée.

80 Le Conseil sur l'intelligence artificielle est un Groupe d'experts créé par le Comité de la politique de l'économie numérique de l'OCDE en mai 2018. Il est chargé d'élaborer des principes à mettre en œuvre dans le cadre des politiques publiques et de la coopération internationale et a pour vocation de promouvoir la confiance dans l'intelligence artificielle et son adoption.

81 Pour un résumé des différentes positions en doctrine suisse, voir FLÜCKIGER, pp. 853 ss.

82 ROUVROY, p. 19 ; dans une veine similaire, ZUBOFF précise que les mesures de surveillance mises en place par des particuliers comme p. ex. *Google Inc.*, n'ont pas pour but d'anéantir le droit à la sphère privée, mais plutôt de le redistribuer (*The work of surveillance, it appears, is not to erode privacy rights but rather to redistribute them. Instead of many people having some privacy rights, these rights have been concentrated within the surveillance regime. Surveillance capitalists have extensive privacy rights and therefore many opportunities for secrets. These are increasingly used to deprive populations of choice*), voir ZUBOFF, Big Other, p. 83.

traitements se rapportant à la vie privée)[83]. De plus, on rappellera que le droit à l'autodétermination en matière informationnelle a toujours été considéré comme le droit fondamental le plus à même à répondre aux développements technologiques[84]. Au vu de ces développements ainsi que dans un souci de brièveté, la présente contribution ne se penchera que sur la protection offerte par l'art. 13 al. 2 Cst.

Effectuer un profilage n'est pas uniquement envisageable au stade de la procédure d'embauche. De multiples décisions tout au long de la relation de travail peuvent être fondées sur un profilage des employés, comme p. ex. celle de savoir, dans le contexte de licenciements prévus lors d'un projet de fusion, quels employés sont les moins productifs[85]. À l'heure où ces lignes sont rédigées, la pandémie du Covid-19 bat son plein. Le profilage est de plus en plus utilisé par les employeurs suisses qui souhaitent évaluer l'efficacité de leurs employés en télétravail[86]. Toutefois, il semblerait que le plus grand risque d'atteintes à la personnalité et à divers droits fondamentaux se pose au stade précontractuel de la relation de travail, c'est-à-dire pendant la procédure d'embauche. En effet, les dispositions ayant pour but de protéger la personnalité de l'employé pendant une relation de travail ne s'applique que dans certaines limites (peu claires) avant la conclusion du contrat[87]. En d'autres termes, les relations précontractuelles sont (encore) moins encadrées que les relations de travail. Le Législateur considère qu'à ce stade précontractuel, les deux futures parties au contrat de travail – contrat qui se caractérisera par un lien de subordination – se trouvent (encore) sur un pied d'égalité[88]. Si cette approche semble justifiée d'un point de vue abstrait, elle ne semble toutefois pas refléter la dynamique entre recruteurs

83 FLÜCKIGER, pp. 846 s. ; dans le même sens à propos du droit « constitutionnel » européen, voir KOKOTT/SOBOTTA, p. 225.

84 HERTIG RANDALL/MARQUIS, art. 13 al. 2 Cst., N 63 ; DIGGELMANN, art. 13 al. 2 Cst., N 32.

85 O'NEIL, pp. 132 ss. ; MORGENROTH, p. 156.

86 PFPDT, 28e rapport d'activités, p. 48 ; KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, pp. 79 ss. ; même si la Suisse ne fait pas partie des pays figurant dans le rapport de *vmware*, les résultats de ce sondage effectué en juillet et août 2021 devraient également refléter la tendance en Suisse, voir vmware, The Virtual Floorplan, New Rules for a New Era of Work, p. 12 ; cette thématique a également fréquemment été abordée dans la presse suisse et étrangère, à titre d'exemple, voir WASSMER, Télétravail : la tentation de la surveillance ou GRATWOHL/RÜTTI, Big Brother im Home-Office : Das Vertrauen der Mitarbeiter steht auf dem Spiel.

87 MATHIS-ZWYGART, pp. 311 s.

88 STAEHELIN part du principe que les parties négocient sur un pied d'égalité dans la mesure où il précise que les négociations sont régies par le principe de la *culpa in contrahendo*, voir STAEHELIN, art. 320 CO, N 33 ; pour une analyse plus différenciée quant à une possible application des dispositions protégeant la personnalité de l'employé au stade de la procédure d'embauche également, voir DUNAND, art. 328b CO, N 5.

et candidats souvent observée en pratique[89]. Dans un souci de brièveté, cette contribution ne se penchera pas sur l'utilisation du profilage ni pendant ni après la relation de travail. Ce choix ne devrait toutefois pas être interprété comme l'affirmation selon laquelle les employés sont suffisamment protégés contre de possibles utilisations abusives de leurs données personnelles tout au long de leur relation de travail ainsi qu'une fois qu'ils ont quitté l'entreprise. En d'autres termes, ce choix ne nie en aucun cas le fait que dans ces contextes aussi, des mesures attentatoires à l'autodétermination en matière informationnelle des (ex-)employés peuvent être mises en œuvre.

Par ailleurs, cette contribution n'analysera pas le cadre légal d'un profilage effectué dans le cadre d'une procédure d'embauche soumise au droit public (cantonal ou fédéral). D'une part, ces procédures sont soumises au droit cantonal lorsque les personnes concernées souhaitent travailler pour un organe cantonal, voire communal. Dans un souci de brièveté, j'ai décidé de ne pas me pencher sur les 26 droits cantonaux différents. D'autre part, en vertu du principe de légalité, le recours au profilage par les organes fédéraux doit pouvoir se fonder sur une loi au sens formel[90]. Dès lors, si les organes fédéraux souhaitaient recourir au profilage dans le cadre d'une procédure d'embauche, une base légale devrait être adoptée. À défaut d'une telle disposition, le recours au profilage constituerait un traitement de données illicite. En raison de ce qui précède, le profilage au niveau fédéral pose moins de problème : il ne saurait se faire à l'insu des personnes concernées[91]. Les risques liés au profilage sont donc plus petits que dans le secteur privé où la liberté des employeurs, quant aux traitements des données personnelles des candidats, est considérablement plus grande[92].

Souvent faussement qualifié de profilage, le cadre légal de simples recherches sur Internet à l'aide de moteurs de recherche ou sur les réseaux sociaux ne sera pas non plus analysé dans cette contribution[93].

---

89 À titre d'exemple, voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 62 ou TRUTMANN, p. 472.

90 Art. 5 al. 1er Cst. dont l'art. 34 al. 2 let. b LPD se fait l'écho en matière de traitements de données.

91 L'Ordonnance concernant la protection des données personnelles du personnel de la Confédération du 22 novembre 2017 (OPDC, RS 172.220.111.4) règle, entre autres, le traitement des données personnelles des candidats à un emploi. Les art. 12 à 18 OPDC fixent le cadre légal du système d'information pour le recrutement des collaborateurs. À l'heure actuelle, un profilage des candidats à la fonction publique fédérale n'est pas prévu.

92 Pour une comparaison plus générale allant dans le même sens (risques liés aux traitements de données effectués par des particuliers vs. risques liés aux traitements effectués par des organes publics), voir JÖHRI, N 8.100.

93 Pour une analyse du cadre légal de ces évaluations *non*-automatisées de certains aspects de la personnalité des candidats, voir, à titre d'exemple, EGLI, pp. 18 ss. ; DUNAND fait référence à cette « pratique courante » en utilisant la notion de *screening*, voir DUNAND, art. 328b CO, N 59 ; pour des références supplémentaires, voir LEMPEN, pp. 282 ss.

Il en va de même des systèmes de notation qui fonctionnent sur la base de profilages. Ainsi, à titre d'exemple, l'entreprise américaine *Uber* demande à ses clients de noter chaque chauffeur une fois la course terminée. Ces notations sont ensuite utilisées par *Uber* pour prendre certaines décisions de gestion d'entreprise par rapport aux chauffeurs. Bien qu'il s'agisse de profilage dans le contexte du travail, ces notations sont le fruit d'une évaluation automatisée de la relation entre le client et le chauffeur[94]. Même s'il est avéré que cette notation a un effet sur la relation entre l'employeur *Uber* et l'employé chauffeur[95] et qu'il est vrai que dans ce contexte se posent également plusieurs questions relatives aux droits fondamentaux[96], cette contribution se limitera à l'analyse d'une des multiples conséquences de la numérisation sur la relation entre l'employeur et l'employé à proprement parlé. L'impact d'un profilage d'un indépendant/employé par un client ne sera donc pas abordé dans cette contribution. Dans une veine similaire, un éventuel profilage effectué lors d'un placement privé de personnel ou d'une location de services ne sera pas étudié dans le cadre de cette contribution. À ce sujet, on rappellera que les traitements de données effectués dans ce contexte sont soumis à une législation spéciale[97].

Enfin, il convient de noter que cette contribution ne se penchera pas sur les éventuelles questions qui se posent en matière de droit de la concurrence. En effet, certains auteurs ont fait valoir qu'une des mesures permettant de minimiser les risques liés au profilage constituerait à éviter, par le biais du droit de la concurrence, que quelques entreprises détiennent une quantité aussi importante de données personnelles (et non-personnelles)[98]. De même, les

94 KAUFMANN/SCHUERCH, Positionspapier, p. 4.

95 Qualification juridique reprise de l'arrêt du Tribunal fédéral 2C_34/2021 du 30 mai 2022 venant clarifier cette question en droit suisse.

96 BODIE/CHERRY/MCCORMICK/TANG, p. 1027 avec davantage d'exemples et de références.

97 Les traitements de données qui peuvent être effectués lors d'un placement privé de personnel ou d'une location de services sont régis par la Loi fédérale sur le service de l'emploi et la location de services (LSE) du 6 octobre 1989, RS 823.11 et l'Ordonnance sur le service de l'emploi et la location de services (OSE) du 16 janvier 1991 (RS 823.111) et, plus précisément, par les art. 7 al. 3 LSE et 19 OSE ainsi que les art. 18 al. 3 LSE et 47 OSE. Étant donné que ces traitements soulèvent de nombreuses questions en pratique, le PFPDT a apporté des précisions quant à quelques-unes de ces questions, voir PFPDT, Guide pour le traitement des données personnelles dans le secteur du travail, Traitements par des personnes privées, 2 octobre 2014, pp. 8 ss.

98 À titre d'exemple, ELIZABETH WARREN, candidate aux primaires présidentielles du Parti démocrate en 2020, avait inclus de telles propositions dans son programme électoral (voir WARREN E., How We Can Break Up Big Tech ; pour une analyse plus réservée quant au champ d'application du droit de la concurrence suisse, voir WEBER, p. 21 ; pour un avis contraire dans la mesure où même la mise en œuvre de mesures anti-concurrentielles ne garantirait pas une meilleure protection des droits des individus, voir ZUBOFF, Surveillance Capitalism, pp. 14, 23 et 193.

éventuelles questions qui se posent en matière du droit de la propriété intellectuelle ne feront pas l'objet de l'analyse qui suit[99]. Pour une approche empirique à la thématique, on consultera les publications d'auteurs qui ont pris le temps de contacter certains employeurs en Suisse ou à l'étranger (avec des résultats très hétérogènes)[100]. Il en va de même pour les aspects *strictement* procéduraux du profilage[101].

Afin de mener à bon port les développements qui suivent, il convient, dans une première partie, de définir les notions et concepts clés utilisés tout au long de cette contribution avant d'analyser le cadre légal prévu par les diverses lois fédérales suisses dans une deuxième partie. Cette analyse permettra de déterminer dans quelle mesure un profilage effectué au stade de la procédure d'embauche est licite et si ce cadre légal garantit une protection efficace des droits des candidats. Enfin, la troisième partie sera consacrée à la portée (potentielle) du droit fondamental à l'autodétermination en matière informationnelle entre particuliers, notamment dans le cadre d'une procédure d'embauche. Cette contribution se terminera par un dernier chapitre qui offrira un résumé des mesures juridiques qui pourraient contribuer à mieux encadrer le profilage d'une personne candidate en Suisse. La conclusion permettra de résumer l'analyse et d'esquisser quelques perspectives.

99 Pour un très bref aperçu des spécificités du régime de protection applicable aux logiciels, voir MÉTILLE, Internet et droit, p. 128.

100 KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, pp. 7 et 51 ss., qui n'ont malheureusement pas publié leurs résultats exacts, mais se contentent de les discuter dans le cadre de l'analyse juridique ; pour la première étude empirique suisse portant sur les différentes formes de *People Analytics*, voir WILDHABER/KASPER, Quantifizierte Arbeitnehmer, pp. 760 ss., dont les résultats permettent une appréciation de la situation en Suisse en fonction de la taille de l'entreprise, du secteur économique concerné, du stade de la relation contractuelle concerné et des formes de profilage mis en place ; pour une étude menée en pleine pandémie révélant, entre autres, que 70% des employeurs contactés avaient mis en place ou envisageaient de mettre en place des nouvelles mesures de surveillance *pendant* la relation de travail, voir vmware, The Virtual Floorplan, New Rules for a New Era of Work, octobre 2021, p. 12 ; pour une évaluation empirique peu après l'entrée en vigueur de l'aLPD et de l'art. 328b CO, voir RUDOLPH, Stellenbewerbung und Datenschutz, pp. 158 ss. Dans ce contexte, RUDOLPH souligne qu'en 1995, les employeurs semblaient exercer plus de retenue qu'en 1985 (date à laquelle HUBER avait dédié sa thèse soutenue à l'Université de Zurich à cette même question) quant aux traitements de données effectués pendant la procédure d'embauche. Il estime cependant qu'un lien entre l'entrée en vigueur de l'art. 328b CO et de l'aLPD ne peut qu'être supposé et non prouvé, voir idem, p. 166. Comme le montrent les rapports récents, cette tendance a été renversée avec l'avènement du *Big Data*.

101 Pour les aspects procéduraux du droit d'accès qui permet à la personne concernée de vérifier que les données traitées sont exactes et traitées de manière conforme aux dispositions légales avant d'exercer, le cas échéant, ses droits, voir, à titre d'exemple, BENHAMOU, pp. 77 ss. ; à juste titre, SCHWEIZER rappelle que les prétentions fixées à l'art. 32 LPD trouvent leur fondement, au niveau international, à l'art. 13 CEDH et cite ainsi la jurisprudence pertinente, voir SCHWEIZER R., art. 13 al. 2 Cst., N 47.

Partie 1. Notions et concepts clés

À juste titre, le WEF précise, dans son rapport publié en 2014, qu'« [traduction] avant que la confiance dans l'utilisation des données personnelles puisse être renforcée de manière significative, un dialogue plus efficace est nécessaire. Le dialogue actuel a été façonné par l'utilisation de termes vagues et imprécis qui précèdent généralement le mot 'données' ». Cette constatation est également vraie en matière de profilage. Ainsi, dans le but de mener la discussion qui suit à bon port[102], il est nécessaire, dans un premier temps, de reprendre l'exemple cité en guise d'introduction et de rappeler tant les points communs que les différences entre la surveillance mise en place par les autorités publiques et celle, moins connue, mise en place par des particuliers (chapitre 1) avant de circonscrire le traitement de données connu sous le nom de « profilage » (chapitre 2). Afin de saisir l'ampleur potentielle de cette nouvelle forme de surveillance, il est important de se pencher sur quelques contextes dans lesquels il peut être envisagé d'effectuer un profilage (chapitre 3) avant de clore cette première partie par un aperçu des chances et des risques de ce nouveau traitement de données effectué lors d'une procédure d'embauche (chapitre 4).

102 WEF, p. 15.

Chapitre 1. D'une surveillance publique à une surveillance privée

Le plus souvent, les critiques en matière de protection des données sont émises à l'encontre des autorités publiques[103]. Or, c'est précisément la valeur des données plus ou moins volontairement divulguées par et sur les individus – p. ex. pour des campagnes de marketing ou des employeurs potentiels – qui remet en cause le droit fondamental à l'autodétermination en matière informationnelle (dans les relations entre particuliers)[104]. Dans le but de mieux comprendre les enjeux, il est essentiel de comparer les traitements de données effectués par les autorités publiques et ceux mis en place par des particuliers. Ainsi, reprenant l'exemple cité en guise d'introduction, les prestations offertes par les entreprises comme *Crystal Knows* ressemblent, de prime abord du moins, à la pratique des fiches. Si quelques points communs peuvent en effet être relevés (A), force est de constater que ces deux formes de surveillance divergent sur de nombreux points importants (B).

A. Les points communs

Pour le sociologue DAVID LYON, la notion de surveillance décrit une collecte de données personnelles qui est suivie d'un autre[105] traitement dans le but de contrôler et influencer des individus[106]. Ainsi, il convient de relever que les activités des autorités fédérales et cantonales dénoncées à la fin des années 1980 et les services offerts par des entreprises privées telles que *Wepow*, *HireRight* ou *Crystal Knows* peuvent se résumer à une collecte suivie d'un deuxième traitement desdites données dans le but de contrôler certains individus (identifier

103 Pour un aperçu de publications allemandes dans lesquelles les auteurs défendent l'idée que la surveillance publique est plus « dangereuse » que la surveillance exercée par des particuliers, voir FASNACHT, N 116 ; pour une analyse américaine qui met en garde contre la tendance de certains activistes d'adresser leurs critiques uniquement à l'encontre des mesures de surveillance mises en place par les autorités, voir PASQUALE, The Other Big Brother.

104 STREINZ/MICHL, pp. 384 s.

105 On rappellera qu'en vertu de la LPD, la collecte constitue un traitement de données. Juridiquement, le traitement effectué sur la base des données collectées est un deuxième traitement distinct de la collecte, voir art. 5 let. d LPD.

106 LYON tel que cité dans BÜCHI et al., p. 6.

les menaces communistes au sein de la population, voire identifier le meilleur candidat pour un poste déterminé). Dès lors, le premier point commun à relever porte sur le fait qu'il s'agit d'une forme de surveillance dans les deux cas de figure[107].

Ensuite, une personne fichée, respectivement profilée, pourra subir des désavantages sur le marché du travail sans connaissance de cause.

Par ailleurs, les deux formes de surveillance se fondent sur des critères d'évaluation inconnus. En d'autres termes, même dans l'hypothèse où une personne concernée aurait connaissance du profilage ou de sa fiche, elle ne disposait, respectivement ne dispose pas de moyens lui permettant de rectifier la conclusion erronée. En effet, en l'absence de base légale qui aurait fixé les critères justifiant une mesure de surveillance, il n'était souvent que peu clair selon quels critères une fiche était ouverte[108]. De même, en raison de l'opacité des algorithmes utilisés lors de l'évaluation des données collectées, même les entreprises offrant des services de profilage ne peuvent pas suivre le raisonnement qui sous-tend l'évaluation[109]. En d'autres termes, même lorsque la personne a connaissance de la mesure de surveillance, elle n'avait, respectivement n'aura pas la possibilité de comprendre le raisonnement qui sous-tend l'évaluation faite et d'ainsi pouvoir la remettre en question si elle s'avérait désavantageuse à son égard.

De surcroît, l'évaluation désavantageuse peut s'avérer non pas ponctuelle et donc affecter une procédure d'embauche précise, mais plutôt se révéler être de nature permanente, p. ex. dans l'hypothèse où une des données figurant soit dans la fiche soit dans une des multiples bases de données consultée est erronée ou mal interprétée. Dans ce cas de figure, la personne concernée n'avait, respectivement n'aura pas la possibilité de corriger l'information erronée, voire la fausse interprétation qui aura pu en être faite vu le caractère secret de ces évaluations. Ainsi, l'évaluation désavantageuse risque d'être de nature permanente et affecter plusieurs procédures d'embauche et donc l'accès au marché du travail en général[110].

Malgré ces points en commun, la surveillance publique d'une part et la surveillance privée d'autre part se distinguent toutefois sur de nombreux points.

107 BÜCHI et al., p. 22.

108 FF 1990 I 842.

109 O'NEIL, p. 8.

110 Dans le même sens, en 2004 déjà, à propos d'une éventuelle utilisation généralisée de tests génétiques dans le cadre de procédures de recrutement, voir MUND, pp. 192 s. avec des références supplémentaires ; dans le même sens à propos des profilages en général, voir O'NEIL, p. 134.

B. Les points divergents

D'abord, au 20ème siècle, la surveillance était de nature publique (à quelques exceptions près) et donc menée par des agents fédéraux ou cantonaux qui avaient pour mission d'atteindre certains objectifs de nature politique (garantir la sécurité intérieure et extérieure de la Confédération)[111]. Aujourd'hui, un nombre grandissant d'entreprises privées détiennent des bases de données considérables sur un nombre important de citoyens suisses[112]. Les règles qui gouvernent les actions de l'État suisse dans le cadre de la protection de la population contre les différentes menaces à la sécurité publique ne sauraient être appliquées telles quelles aux entreprises privées procédant à la collecte puis à l'évaluation de données non pas dans un but politique, mais commercial[113]. Dans ce contexte, certains auteurs font valoir que cette différence de régime juridique se justifierait par le fait que seules les autorités publiques disposent du monopole de la puissance publique et peuvent donc emprisonner un individu à la suite d'un traitement de données. Dès lors, la surveillance étatique serait plus attentatoire aux droits fondamentaux que la surveillance privée[114]. Dans la même veine, ces auteurs font valoir que si un employé n'apprécie pas les mesures de surveillance sur son lieu de travail, il est libre de changer d'emploi.

111 FF 1990 I 769 s.

112 Pour des exemples suisses, voir FONTI, pp. 34 ss. ou BRISTKO/SCHOOP/WENGER/LEMCKE, Wer sind wir im Internet ? Wir haben den Test gemacht – mit irritierendem Ergebnis ; pour des exemples d'entreprises allemandes détenant de nombreuses données personnelles de citoyens allemands, voir MORGENROTH, pp. 22 ss.

113 La nécessité d'adopter une approche différente en fonction du but poursuivi lors du traitement de données a été reconnue par le Législateur européen dans la mesure où le Règlement général sur la protection des données vient protéger les personnes physiques à l'égard du traitement de données à caractère personnel. Toutefois, son champ d'application est limité aux activités relevant du marché intérieur et à celles des autorités publiques autres que les autorités répressives. L'adoption d'un instrument spécifique s'est donc imposée afin de parvenir à la clarté et à l'équilibre nécessaires entre la protection des données et les intérêts des autorités répressives. À cette fin, la Directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des actions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données a été adoptée le 27 avril 2016. Cela étant, depuis les « révélations Snowden », il est évident que les services de renseignement collaborent étroitement avec les entreprises privées qui collectent puis traitent une quantité considérable de données personnelles, voir, à titre d'exemple, LYON, p. 2 ou PASQUALE, Black Box Society, pp. 50 s. Pour des raisons de brièveté, cette collaboration publique-privée ne fera toutefois pas l'objet de cette contribution.

114 Pour un aperçu de publications allemandes dans lesquelles les auteurs défendent l'idée que la surveillance publique est plus « dangereuse » que la surveillance exercée par des particuliers, voir FASNACHT, N 116.

En d'autres termes, ils affirment qu'un changement de pays de résidence en raison de mesures de surveillance publique problématiques serait considérablement plus compliqué que de changer d'emploi. Or, ces auteurs méconnaissent le fait qu'en raison du lien de subordination qui caractérise la relation de travail, il peut s'avérer particulièrement difficile de faire valoir ses droits sur le lieu de travail, voire dans le cadre d'une procédure d'embauche. De plus, avec une pression concurrentielle grandissante, des transferts de données de plus en plus faciles et des évaluations de plus en plus précises et de moins en moins coûteuses, changer d'emploi risque de ne pas permettre à un employé concerné par des mesures de surveillance de mieux faire respecter ses droits[115]. Les deux formes de surveillance peuvent porter atteinte à divers droits fondamentaux et méritent dès lors d'être encadrées par un régime qui tient compte des spécificités de chacune de ces formes de surveillance.

Ensuite, la surveillance étatique, du moins au 20ème siècle, s'intéressait avant tout aux données personnelles au sens de la Loi sur la protection des données (ci-après « LPD »). En effet, les services de renseignement et la police fédérale s'intéressaient à toutes les informations concernant une personne physique identifiée ou identifiable[116]. En d'autres termes, l'intérêt pour les métadonnées[117], voire pour les données anonymes n'est que récent et est entre autres dû au développement de l'intelligence artificielle[118]. Ainsi, la surveillance étatique « traditionnelle » et la surveillance privée portent souvent, mais pas toujours, sur les mêmes catégories de données.

Ces deux formes de surveillance se distinguent également quant au processus de générer de nouvelles informations. Avant l'avènement de l'intelligence artificielle, les autorités s'intéressaient aux liens de causalité entre un fait et sa possible conséquence (p. ex. une participation dans un syndicat impliquait souvent un certain point de vue politique). Aujourd'hui, l'intelligence artificielle a pour but de déceler des corrélations entre deux informations (p. ex. l'intérêt

115 À juste titre, PASQUALE contredit la position de ces auteurs, voir PASQUALE, The Other Big Brother.

116 Art. 5 let. a LPD.

117 Les métadonnées sont les « données qui procurent des informations par rapport à d'autres données », p. ex. la date et l'heure à laquelle un site est visité ou encore combien de fois par jour une certaine application est consultée par une même personne. Le contenu d'un message n'est donc pas une métadonnée, voir la définition proposée par CHRISTL/SPIEKERMANN, p. 16.

118 Pour un exemple d'une étude suisse qui a pu déterminer, grâce à de l'intelligence artificielle, des corrélations entre certaines métadonnées générées lors de l'utilisation d'un téléphone mobile (p. ex. nombre d'appels manqués, longueur moyenne des mots envoyés, applications les plus fréquemment utilisées etc.) et certains traits de la personnalité, voir CHITTARANJAN et al., pp. 433 ss.

pour les mangas japonais est souvent corrélé à un certain talent pour la programmation) sans pour autant chercher à comprendre ce lien de corrélation[119]. Ainsi, la logique qui sous-tend ces deux formes de surveillance se distingue fondamentalement et entraîne de nombreuses conséquences juridiques qu'il conviendra de mettre en avant dans cette contribution.

Par ailleurs, aujourd'hui, toute personne active sur le marché du travail peut apparaître dans une base de données exploitées par un *data broker* et donc être soumise à une forme de surveillance privée. Afin de figurer dans une des multiples bases de données dépouillées par les entreprises procédant au profilage de candidats, il n'est pas même nécessaire de posséder un téléphone portable ou s'être naïvement aventuré dans les méandres de l'Internet. Il peut suffire d'avoir une carte client utilisée à d'autres fins que celle de collecter des points fidélités, être la victime d'une attaque cyber ou figurer dans une ou plusieurs bases de données publiques mises à disposition par les autorités compétentes. Le nombre de victimes potentielles de surveillance privée est donc plus important aujourd'hui qu'autrefois lorsque les gouvernements fédéraux et cantonaux surveillaient « uniquement » les citoyens considérés constituer une menace communiste[120].

Ensuite, la surveillance publique s'intéressait non seulement aux individus, mais aussi aux associations, aux partis politiques, aux syndicats et à tout autre groupement qui pouvait être considéré comme une menace pour l'ordre public suisse. La surveillance privée telle que pratiquée aujourd'hui s'intéresse avant tout à classer des individus dans des catégories de plus en plus précises de consommateurs[121], respectivement d'employés. Ainsi, les deux formes de surveillance ne portent pas toujours sur les mêmes sujets de droit.

Subséquemment, devoir suivre une personne sans qu'elle ne s'en rende compte est compliqué, très coûteux et souvent hasardeux. De plus, la surveillance étatique s'arrêtait souvent aux portes de l'appartement des personnes concernées. Aujourd'hui, la surveillance est simple, peu coûteuse et permanente[122]. L'ampleur de la surveillance privée diffère donc aujourd'hui également de l'ampleur de la surveillance publique à la fin des années 1980.

119 CHRISTL/SPIEKERMANN, p. 12.

120 Dans le même sens à propos des différences entre les mesures de surveillance mises en place par les employeurs et celles mises en place par les services de renseignement, voir PASQUALE, The Other Big Brother.

121 CHRISTL/SPIEKERMANN, p. 9 ; à ce sujet, il convient de relever que récemment, l'efficacité du marketing individualisé semble avoir été remis en cause, voir, à titre d'exemple, FULTERER, Warum Tracking-basierte Werbung überschätzt und auf dem Abschwung ist. Ces publications n'ont pour autant pas (encore) remis en cause le modèle économique de la publicité numérique.

122 BERANEK ZANON, p. 87.

En outre, on rappellera que la surveillance privée est plus simple à mettre en œuvre, simultanément, dans différents pays. Au contraire, les mesures mises en place par les services de renseignement dépendent de décisions politiques nationales et diffèrent ainsi d'un pays à un autre[123]. Ainsi, ces deux formes de surveillance se distinguent également quant aux moyens nécessaires à leur mise en œuvre.

Enfin, à aucun moment les citoyens suisses n'ont consenti, ne serait-ce qu'en approuvant une loi allant dans ce sens, à être surveillés par les pouvoirs publics. Aujourd'hui, du moins d'un point de vue strictement juridique, nous consentons à ce que nous soyons suivis sur Internet, que nos données personnelles soient stockées sur des serveurs et qu'une fois analysées, elles soient vendues puis évaluées par des entreprises tierces que nous ne connaissons pas[124]. Aujourd'hui, nous avons échangé nos données personnelles contre l'octroi de services gratuits. D'un point de vue strictement juridique nous avons donc consenti à la surveillance privée[125], ce qui ne saurait être affirmé dans le contexte de la surveillance de la part des autorités publiques au 20ème siècle.

Il convient de noter qu'il n'existe pas seulement les deux formes de surveillance décrites ci-dessus (État – personne physique; personne morale – personne physique). En effet, afin de mieux contextualiser le débat qui suit, il convient de résumer les différentes formes de surveillance à l'aide du tableau suivant[126] :

123 Cela étant, tous les services de renseignement européens semblent avoir de plus en plus de compétences ; pour une brève analyse de la jurisprudence de la Cour EDH relative aux mesures de surveillance mises en place par le gouvernement du Royaume-Uni dans le cadre de la lutte contre le terrorisme et une appréciation critique de la LRens révisée suisse, voir HERTIG RANDALL/MARQUIS, art. 13 al. 1er Cst., N 57 ss.

124 À titre d'exemple, l'agence de publicité zurichoise *Converto* a mis en place une campagne de publicité pour le supermarché *Denner*. Les internautes qui visitaient certains sites choisis, comme p. ex. ‹www.bluewin.ch› ou ‹www.blick.ch›, et qui voyaient une publicité de légumes frais de *Denner* s'afficher sur leur écran étaient identifiés sans même qu'ils en aient conscience. Grâce à sa collaboration avec la *Poste*, *Converto* a pu identifier les internautes ayant vu la publicité en question et leur envoyer des bons de réduction pour des légumes achetés chez *Denner* à la maison, voir CETOJEVIC/MESCHENMOSER, Vom Bildschirm bis vor die Haustür verfolgt.

125 Pour une analyse critique quant à la validité de ce consentement, voir ZUBOFF, Big Other, p. 82.

126 Repris puis traduit de BÜCHI et al., p. 22.

Figure 1 : Les différentes formes de surveillance d'après BÜCHI et al.

	L'État	Les personnes morales	Les personnes physiques
L'État	Espionnage, services de renseignement	Surveillance de l'industrie, audit, partenariats publics-privés	Traçage (p. ex. « affaire des fiches », programme américain « PRISM »)
Les personnes morales	Lobbying, suivi des décisions	Espionnage industriel	Profilage[127]
Les personnes physiques	Piratage informatique, sousveillance (sic) (p. ex. Anonymous)	Protection des consommateurs, ONG agissant à l'encontre des entreprises (p. ex. AlgorithmWatch ; Privacy International ; nyob)	Stalking

Chapitre 2. La définition compliquée du profilage

Le profilage est un nouveau traitement de données, qui est complexe d'un point de vue de la technologique utilisée et qui peut potentiellement être exploité dans des contextes très divers. Par conséquent, le profilage est difficile à circonscrire juridiquement. Dès lors, il convient de très brièvement expliquer le mode de fonctionnement de cette forme de traitement de données (A) avant de se pencher sur les différentes définitions juridiques qui ont pu être adoptées et qui sont potentiellement applicables en Suisse (B).

A. Le processus du profilage

Malgré les progrès technologiques et l'influence grandissante des entreprises promettant, dans un premier temps, d'être en mesure d'évaluer les données personnelles d'une multitude d'individus afin de prédire, dans un deuxième temps, le comportement, voire la performance de personnes[128], le Parlement

127 On notera que sur ce point, ce tableau ne reflète pas exactement le régime légal suisse. En effet, en vertu des art. 5 let. f et g LPD et 34 al. 2 let. b LPD, les organes fédéraux peuvent également effectuer un profilage.

128 Pour un très bref résumé des développements technologiques de la fin du 18e siècle à nos jours, voir HEUBERGER, N 10 ss. ; pour un résumé des développements de ce secteur économique au niveau mondial depuis les années 1970, voir CHRISTL/SPIEKERMANN, pp. 76 ss. ; pour un bref aperçu des développements des activités des courtiers en données aux États-Unis, voir Commissariat à la protection de la vie privée au Canada, pp. 2 ss.

suisse n'a adopté une définition de cette forme de traitement de données connue sous le nom de profilage qu'en automne 2020. Avant l'entrée en vigueur de cette définition le 1er septembre 2023, les traitements de données connus désormais sous le nom de profilage sont certes déjà effectués, mais sans être définis juridiquement ou spécifiquement encadrés[129] par l'ancienne Loi sur la protection des données du 19 juin 1992[130] (ci-après « aLPD »). Les contours exacts de cette nouvelle définition n'ont, bien évidemment, pas encore été déterminés par le Tribunal fédéral[131].

Avant d'analyser les différentes définitions juridiques du profilage potentiellement applicables en Suisse, il convient de clarifier la notion en se fondant sur les travaux de HILDEBRANDT, qui a été une des premières juristes à se pencher sur les enjeux du profilage et qui, en 2008 déjà, a décrit ce nouveau traitement de données de la manière suivante :

> « [traduction] Le profilage décrit le processus qui permet de découvrir des corrélations entre des données figurant dans des bases de données (différentes). Ces corrélations permettent ensuite d'identifier et de représenter un sujet humain ou pas (un individu ou un groupe) et/ou d'appliquer un profil (un ensemble de données corrélées) afin d'individualiser et représenter un sujet ou afin d'identifier un sujet en tant que membre d'un groupe ou d'une catégorie »[132].

Dans son Exposé des motifs annexé à sa Recommandation dédiée au profilage[133] publiée deux ans plus tard, le Comité des Ministres du Conseil de l'Europe

129 Pour quelques exemples tirés de la pratique de la fin des années 2000, voir WALTER, Le profilage, pp. 88 s.

130 Loi fédérale sur la protection des données du 19 juin 1992 (LPD), RS 235.1. Pour une explication de la raison pour laquelle l'aLPD n'encadrait cette forme de traitement de données que de manière incomplète, le Message du Conseil fédéral précise que « compte tenu des nouvelles technologies, les données peuvent aujourd'hui être exploitées comme un fichier, alors même qu'elles sont disséminées. Un exemple parlant est le profilage, lors duquel on va chercher des données dans différentes sources, non constitutives de fichiers, afin d'évaluer certaines caractéristiques d'une personne. Selon le droit actuel [aLPD], ces activités échappent aux dispositions de la loi impliquant la présence d'un fichier, comme le droit d'accès [art. 8 aLPD] ou le devoir d'information [art. 14 aLPD], alors que ce sont justement les situations de ce type qui nécessitent une plus grande transparence », voir FF 2017 6643 s. ; dans le même sens, voir HEUBERGER, N 54 et (de manière moins explicite) KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 46.

131 Pour une analyse approfondie des insécurités juridiques liées à la définition du profilage qui subsistent, voir *infra* Chapitre 2. La définition compliquée du profilage et Chapitre 8. La Loi sur la protection des données.

132 HILDEBRANDT, p. 19.

133 La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, Recommandation CM/Rec(2010)13 adoptée par

semble reprendre (en partie) la description en trois temps de HILDEBRANDT en précisant que « le profilage [...] se déroule en trois étapes techniquement distinctes :

— une étape de collecte et d'entreposage massifs (*data warehousing*) des observations numérisées des comportements et caractéristiques des individus. Ces observations peuvent être nominatives, codées ou anonymes ;
— une étape d'analyse et de « forage » (*data mining*) de ces données permettant l'établissement de corrélations entre certains comportements/caractéristiques et d'autres comportements ou caractéristiques ;
— une étape d'inférence au cours de laquelle, à partir de certaines variables comportementales ou caractéristiques observables propres à un individu généralement identifié, de nouvelles caractéristiques ou variables comportementales présentes, passées ou futures, sont déduites »[134].

Ainsi, le profilage est un processus inductif qui a pour but de créer de nouvelles connaissances sur la base d'informations déjà disponibles, notamment en calculant des corrélations avant d'appliquer ces corrélations à des individus[135]. En des termes moins abstraits, le profilage vise à évaluer certains aspects de la personnalité d'une personne physique afin de lui offrir un service individualisé ou à calculer le risque potentiellement encouru si une relation juridique est entamée avec cette même personne[136]. Ce processus caractéristique du *Big Data* se distingue de manière fondamentale de l'approche déductive qui caractérise les sciences sociales. À cet égard, ROUVROY précise que « [traduction] plutôt que de subsumer les données dans des catégories préétablies (telles que des catégories statistiques, dont la mise en place nécessite un processus conventionnel potentiellement long), le traitement de type *Big Data* produit des catégories à partir de l'énorme volume de données lui-même, pratiquement en temps réel. Ces catégories algorithmiques, également appelées modèles ou profils (lorsqu'il s'agit de comportements humains), sont des schémas dynamiques (le terme de visualisation de données est également utilisé) formés à partir de corrélations observées non pas dans le monde physique mais parmi les données numériques collectées dans divers contextes, indépendamment de toute explication causale. En d'autres termes, contrairement au traitement

le Comité des Ministres du Conseil de l'Europe le 23 novembre 2010 et exposé des motifs. On notera que cette recommandation a été révisée en novembre 2021.

134 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 38 ; pour de plus amples informations quant à ces trois éléments et quelques exemples, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 96 ss.

135 BÜCHI et al., p. 4 avec davantage de références.

136 CHRISTL/SPIEKERMANN, p. 13.

statistique classique, dans lequel les hypothèses ou catégories statistiques précèdent et régissent la collecte des données, dans le traitement de type *Big Data*, c'est exactement le contraire qui se produit : la collecte et le traitement des données viennent en premier et font naître des hypothèses ou des catégories dans la masse des données »[137]. Cette différence d'approche à la création de nouvelles connaissances explique, entre autres, les difficultés à définir juridiquement ce nouveau traitement de données[138].

En guise d'exemple, on peut imaginer un commerçant de vin qui, dans le but de mieux gérer ses stocks, analyse quel client a acheté quel vin. Il ne s'agit alors pas de profilage puisqu'il n'y a pas d'évaluation d'un trait de la personnalité ou une quelconque prédiction d'un comportement futur[139]. En revanche, s'il analyse cette banque de données à la recherche de clients qui ont déjà acheté du vin espagnol et qu'il les contacte dans le but de leur vendre du vin espagnol, il y a profilage. En effet, dans le cadre de cette deuxième hypothèse, il évalue un comportement passé afin de prédire un comportement futur[140].

Même si la description du profilage proposée par HILDEBRANDT en 2008 a, par la suite, souvent été citée dans des ouvrages consacrés à ce traitement de données[141], cette définition n'a ni été reprise telle quelle au niveau suisse ni au sein du Conseil de l'Europe ni par les institutions de l'Union européenne (ci-après « UE »). Dès lors, il convient de se pencher sur les définitions juridiques (incomplètes) actuellement en vigueur en Suisse, au sein du Conseil de l'Europe et au niveau de l'UE.

137 ROUVROY, pp. 10 s.

138 Pour des explications plus détaillées quant aux différences entre les traitements de données qui se fondent sur un lien de causalité (même automatisé) et le profilage qui se fonde sur un calcul de corrélations, voir HEUBERGER, N 43 ss.

139 Dans le même sens à propos d'une sélection d'individus sur la base de leurs caractéristiques réelles, le Comité des Ministres mentionne l'exemple suivant : « La sélection, par une banque, des clients riches gagnant plus de dix milles euros par mois et possédant un patrimoine d'au moins un million d'euros constitue une sélection objective qui, au contraire du profilage, n'est pas empreinte d'une marge d'erreur. Techniquement, cette sélection requiert une simple requête sur un serveur *Structured Query Language* (*SQL*) et ne nécessite pas de forage », voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 41.

140 Exemple tel que cité par ROSENTHAL, voir ROSENTHAL, Das neue Datenschutzgesetz, N 26 ; dans le même sens, notamment à propos des *data broker* qui créent des profils précis d'individus sur la base de 1'000 informations et dont les activités seraient un « [traduction] exemple typique de profilage », voir BÜCHI et al., pp. 14 s.

141 À titre d'exemple, voir HEUBERGER, N 59 ; BÜCHI et al., p. 4 ; HÄUSELMANN, N 3.

B. Les différentes définitions juridiques du profilage

Il découle des développements ci-dessus qu'il n'est pas facile de définir le profilage. Les définitions du profilage en droit suisse (1), en droit (révisé) du Conseil de l'Europe (2) et en droit de l'UE (3) se rejoignent certes sur de nombreux points, mais se distinguent sur d'autres. Si quelques conditions sont réunies, tant la définition suisse du profilage que celle prévue en droit de l'UE, voire celle prévue par le Conseil de l'Europe pourraient trouver à s'appliquer en Suisse. Dès lors, il convient de se pencher sur ces différentes définitions.

1. La définition du profilage en droit suisse

Comme mentionné précédemment, aucune définition du profilage ne figurait dans l'aLPD. De même, aucune loi cantonale sur la protection des données ne proposait une définition de ce traitement de données[142]. Sous le régime de l'aLPD, le Tribunal fédéral suisse n'a jamais dû se prononcer par rapport à la notion de profilage. Une définition jurisprudentielle émanant de la plus haute juridiction suisse n'a donc pas précédé la définition légale[143].

La définition adoptée par le Parlement suisse le 25 septembre 2020, qui figure désormais à l'art. 5 let. f LPD, se lit comme suit :

> « On entend par : profilage (sic) : toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

---

142 La Constitution suisse ne consacre pas une compétence exclusive à la Confédération en matière de protection des données. Les cantons restent donc compétents pour la protection des données lorsqu'ils traitent des données personnelles dans un de leurs domaines de compétence. Ainsi, à titre d'exemple, les traitements de données personnelles effectués par les hôpitaux ou les écoles publics sont régis par les lois sur la protection des données cantonales et sont, par conséquent, soumis au contrôle des préposés cantonaux, voir BELSER, § 5, N 42 ss. ; pour un exemple des difficultés de mise en pratique engendrées par ce partage de compétences, voir EPINEY, Abgrenzung, N 1 ss.

143 Il convient de ne pas confondre la notion de « profilage » avec celle de « racial profiling » qui a pu être mentionnée dans quelques arrêts du Tribunal fédéral. En effet, la notion de « racial profiling » telle qu'utilisée dans les arrêts du Tribunal fédéral ne renvoie pas à un traitement de données *automatisé*, mais décrit un comportement potentiellement raciste de la part des forces de l'ordre fondé sur des préjugés, à titre d'exemple, consulter l'arrêt du Tribunal fédéral 6B_1174/2017 du 7 mars 2018, cons. 4.8 dans le cadre duquel le Tribunal fédéral a traduit la notion de « racial profiling » par racisme inconscient (*unbewusster Rassismus*) ; dans le même sens, voir l'arrêt du Tribunal fédéral 6B_869/2020 du 3 septembre 2020 ; pour une analyse de la réception de cette notion en droit suisse, voir NAGUIB, N 5 ss.

Ainsi, le profilage, en droit suisse, se caractérise par les trois éléments cumulatifs suivants :

— un traitement automatisé ;
— de données personnelles (au sens de l'art. 5 let. a LPD) ;
— dans le but d'évaluer certains aspects de la personnalité d'une personne physique.

À ce stade, il est important de noter que le fait d'effectuer une analyse de certains aspects de la personnalité d'une personne physique suffit, afin qu'un traitement de données tombe dans le champ d'application de la définition légale du profilage. Il n'est donc pas nécessaire de procéder à une prédiction du comportement de la personne concernée fondée sur l'évaluation faite, afin d'ouvrir le champ d'application de la LPD[144]. En d'autres termes, cette notion n'englobe uniquement que les hypothèses dans lesquelles il est procédé à une appréciation subjective, qu'il s'agisse d'une analyse d'un comportement précis ou du pronostic d'un comportement. Ainsi, le risque principal du profilage réside dans le fait qu'un aspect (important) de la personnalité d'une personne physique va être évalué non pas par une autre personne physique, mais par une machine[145]. Inversement, la constatation – même automatisée – d'un état de fait ne constitue pas un profilage au sens de la LPD[146].

Ayant conscience que le recours au profilage ne porte pas atteinte à la personnalité des personnes concernées dans toutes les hypothèses[147], le Parlement suisse a décidé d'opérer une distinction entre un profilage, qui ne présente aucun (voire qu'un faible) risque pour la personnalité des personnes concernées et les profilages plus problématiques. Ainsi, l'art. 5 let. g LPD vient définir ce que constitue un profilage à risque élevé. Cette disposition se lit comme suit :

144 « [Le profilage] est défini comme l'évaluation de certaines caractéristiques d'une personne […] afin notamment d'analyser *ou* prédire son rendement au travail […] », voir FF 2017 6642.

145 Pour une analyse plus détaillée des risques liés à l'utilisation du profilage, voir *infra* Chapitre 5. Avantages et risques.

146 ROSENTHAL, Das neue Datenschutzgesetz, N 24 s.

147 Pour un exemple parlant d'un profilage courant, mais sans risque pour la personnalité des personnes concernées, voir l'exemple tel que cité plus haut du marchand de vin qui souhaiterait déterminer lesquels de ses clients apprécient tout particulièrement les vins espagnols, voir ROSENTHAL, Das neue Datenschutzgesetz, N 26 ; dans le même sens, voir MEIER, Big Data, p. 91.

> « On entend par : *profilage à risque élevé* (sic) : tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ».

Ainsi, le profilage à risque élevé se caractérise par les quatre éléments cumulatifs suivants :
- un profilage (au sens de l'art. 5 let. f LPD) ;
- un appariement de données ;
- une appréciation des caractéristiques essentielles de la personnalité d'une personne physique (et non de « certains aspects [non-essentiels] de la personnalité ») ;
- un risque élevé pour la personnalité *ou* les droits fondamentaux de la personne concernée.

Force est de constater que le (nouveau) droit suisse prévoit une définition juridique du profilage et introduit une distinction entre un « profilage général » et un « profilage à risque élevé ». Une telle distinction est inconnue en droit de l'UE. Jusqu'il y a très peu, elle était également inconnue en droit du Conseil de l'Europe. À ce stade, on notera que l'évaluation automatisée des données personnelles d'un candidat est citée comme un exemple de « profilage à risque élevé »[148]. Aussi, on relèvera qu'en droit suisse, le profilage se distingue de la « décision automatisée » telle que définie à l'art. 21 al. 1er LPD. En effet, le nouveau droit suisse circonscrit la décision automatisée de la manière suivante :

> « Toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative ».

Ainsi, la décision automatisée se caractérise par les quatre éléments cumulatifs suivants :
- toute forme de traitement automatisé ;
- de données personnelles ;
- une décision juridique *ou* des effets significatifs sur la personne concernée ;
- aucune intervention humaine.

148 ROSENTHAL, Das neue Datenschutzgesetz, N 27 ; dans le même sens à propos des *smart workplaces* et de l'utilisation de *wearables* sur le lieu de travail (mais non à propos d'un profilage effectué dans le cadre d'une procédure d'embauche), voir KAUFMANN/SCHUERCH, pp. 61 ss., 75 et 79.

Tout comme le profilage, la décision automatisée se limite aux cas dans lesquels une machine prend seule, c'est-à-dire sans intervention humaine[149], une décision qui présuppose une libre appréciation (*Ermessensentscheid*). Ainsi, la décision d'un distributeur de billets de refuser un retrait d'argent allant au-delà de la limite convenue ou un système de contrôle d'accès qui libère l'accès une fois qu'un badge valide est présenté ne constituent pas des décisions automatisées au sens de la LPD[150].

Toutefois, il découle de ce qui précède que malgré leurs points communs, le traitement de données connu sous le nom de « profilage » ne doit, en aucun cas, être confondu avec le traitement de données connu sous le nom de « décision automatisée »[151]. En effet, et reprenant ce qui a pu être dit dans le cadre des délimitations de la présente contribution, un employeur peut effectuer un profilage afin de déterminer certains aspects (essentiels ou non-essentiels) de la personnalité d'un candidat tout en se réservant le droit de prendre la décision – qui se fondera sur l'évaluation automatisée – lui-même. Dans ce premier cas de figure, il n'y a uniquement profilage, mais pas de décision automatisée[152]. À l'inverse, une personne peut mettre en place un algorithme qui va automatiquement prendre une décision (qui présuppose une libre appréciation) sans pour autant procéder à l'évaluation de la personnalité de la personne soumise à la décision automatisée. Dans ce deuxième cas de figure, il y a décision automatique, mais pas de profilage[153]. Enfin, une décision peut être prise de manière automatisée en se fondant sur une évaluation automatisée de certains aspects de la personnalité de la personne concernée. Dans ce troisième cas de

149 FF 2017 6674 ; la doctrine semble confirmer cette condition stricte, voir ROSENTHAL, Das neue Datenschutzgesetz, N 108. On notera que par rapport à la même condition constitutive du profilage, la doctrine se montre plus flexible, voir *infra* Chapitre 8. La loi sur la protection des données.

150 ROSENTHAL, Das neue Datenschutzgesetz, N 107.

151 Pour un exposé du cadre légal et une analyse critique, voir *infra* Chapitre 8. La Loi sur la protection des données.

152 ROSENTHAL estime, à juste titre, qu'il n'y a pas de décision individuelle automatisée au sens de la nLPD lorsqu'un ordinateur propose à un employé de banque des limites de découvert individuelles, mais que celles-ci sont finalement approuvées par l'employé, voir ROSENTHAL, Das neue Datenschutzgesetz, N 108.

153 ROSENTHAL estime que tel serait le cas, par exemple, si un employeur décide de mettre en place un processus automatisé qui ne retient que les candidatures de personnes ayant une certaine moyenne, voir ROSENTHAL, Das neue Datenschutzgesetz, N 107. Notons toutefois que la moyenne obtenue lors d'un examen peut (mais ne doit pas) être un indice par rapport à l'intelligence du candidat. Cette moyenne figurant dans le dossier pourrait alors révéler « un aspect de la personnalité » du candidat. Le traitement automatisé mis en place par l'employeur pourrait alors constituer un profilage au sens de la LPD, pour une analyse plus approfondie de cette distinction complexe entre profilage et décision individuelle automatisée, voir *infra* Chapitre 8. La Loi sur la protection des données.

figure, le responsable du traitement effectuera un profilage puis une décision automatisée. Il convient de noter que le cadre légal régissant les décisions automatisées – qu'elles se fondent ou pas sur une évaluation des traits de la personnalité (profilage) – ne sera pas analysé dans cette contribution. En d'autres termes, les développements qui suivent mettent en lumière le cadre légal (lacunaire) du profilage, qu'il soit suivi d'une décision automatisée ou non[154].

Le profilage peut, dans certains contextes, soulever d'importantes questions par rapport au respect de différents droits fondamentaux. Ainsi, il convient de se pencher sur une éventuelle définition proposée par la Cour européenne des droits de l'homme (ci-après « Cour EDH »), définition qui serait contraignante pour la Suisse. En effet, la Convention européenne des droits de l'homme[155] (ci-après « CEDH ») est directement applicable dans l'ordre juridique suisse[156] et a, par le passé, considérablement influencé les développements législatifs et jurisprudentiels[157].

2. La définition du profilage du Conseil de l'Europe

Depuis un certain temps déjà, différents organes du Conseil de l'Europe ont cherché à savoir comment protéger au mieux la sphère privée (et d'autres droits fondamentaux) des citoyens européens à l'ère du numérique. Même s'il est vrai que les citoyens suisses ne peuvent que se fonder sur la CEDH afin de faire valoir leurs droits, la Cour EDH s'inspire des travaux d'autres organes du Conseil de l'Europe, notamment lorsqu'il s'agit d'apporter une réponse à une problématique nouvelle. Dans ce contexte, on pensera à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère

154 Pour une analyse de la différence entre un profilage et une décision individuelle automatisée en droit suisse, voir ROSENTHAL, Das neue Datenschutzgesetz, N 106 ss. et HEUBERGER, N 185 ss. On notera que le Message reste muet à ce sujet. Le Conseil fédéral se contente de citer quelques exemples de profilage et quelques exemples de décisions individuelles automatisées, voir FF 2017 6642 et 6674 s. ; pour une analyse des différents éléments des définitions d'une décision individuelle automatisée et d'un profilage en droit européen, voir Groupe « Article 29 » sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679. On rappellera que le Groupe « Article 29 » sur la protection des données est l'ancien organe consultatif indépendant de l'UE.

155 Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, approuvée par l'Assemblée fédérale le 3 octobre 1974, RS 0.101.

156 BESSON, Harmoniser le droit privé, p. 9.

157 Pour des exemples d'arrêts du Tribunal fédéral qui ont été considérablement influencés par la jurisprudence de la Cour EDH, voir HÄFELIN/HALLER/KELLER/THURNHERR, N 165. Cette influence est entre autres due au fait que « depuis 1976 déjà, le Tribunal fédéral considère les droits de la CEDH comme des droits constitutionnels à part entière au sens de l'art. 189 al. 1 let. a Cst. », voir BESSON, Humaniser le droit privé, p. 9.

personnel[158] (ci-après « Convention 108 ») ou aux recommandations du Comité des Ministres[159]. Ainsi, il convient de se pencher, d'abord, sur une éventuelle définition jurisprudentielle fondée directement sur une des dispositions de la CEDH (a) avant de consulter les publications d'autres institutions du Conseil de l'Europe qui pourraient, un jour, inspirer la Cour EDH en matière de protection des données, notamment la Convention 108 (b) et la Recommandation relative à la Protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, qui a été révisée en novembre 2021 (c).

a. La Convention européenne des droits de l'homme

Il est de jurisprudence constante que le droit à la protection des données personnelles fait partie des droits protégés par l'art. 8 CEDH[160], qui consacre le droit au respect de la vie privée et familiale. Dans certains contextes, la Cour EDH en a déduit une obligation positive à l'encontre des Hautes parties contractantes, notamment dans une affaire portant sur une mesure de surveillance mise en place sur le lieu de travail[161]. La notion spécifique de « profilage » (soit « profiling » en anglais) n'a cependant été utilisée que dans 25 arrêts de chambre ou de Grande chambre seulement[162]. Il est intéressant de noter que dans la plupart

158 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, approuvée par l'Assemblée fédérale le 5 juin 1997, RS 0.235.1.

159 À titre d'exemple, voir *Barbulescu c. Roumanie* [GC], 5 septembre 2017, n° 61496/08, § 43 ou *López Ribalda et al. c. Espagne* [GC], 17 octobre 2019, n° 1874/13 et 8567/13, § 62.

160 À titre d'exemple, voir *S. et Marper c. Royaume-Uni* [GC], 4 décembre 2008, n° 30562/04 et 30566/04, § 67 qui fixe que « le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'art. 8 CEDH (…). Peu importe que les informations mémorisées soient ou non utilisées par la suite ».

161 *Barbulescu c. Roumanie* [GC], 5 septembre 2017, n° 61496/08, § 141.

162 *S. et Marper c. Royaume-Uni* [GC], 4 décembre 2008, n° 30562/04 et 30566/04, §§ 64 et 73 ; *Stefanou c. Grèce*, 22 avril 2010, n° 2954/07, § 24 ; *Dubetska et al. c. Ukraine*, 10 février 2011, n° 30499/03, § 69 ; *Vladimir Vasilyev c. Russie*, 10 janvier 2012, n° 28370/05, § 17 ; *Fáber c. Hongrie*, 24 juillet 2012, n° 40721/08, Opinion dissidente de la Juge KELLER, § 15 ; *Dembele c. Suisse*, 24 septembre 2013, n° 74010/11, § 30 ; *Géorgie c. Russie (I)* [GC], 3 juillet 2014, n° 13255/07, Opinion séparée de la Juge TSOTSORIA, pp. 70, 71 et 74 ; *Ciorcan et al. c. Roumanie*, 27 janvier 2015, n° 29414/09 et 44841/09, § 76 ; *Szabó et Vissy c. Hongrie*, 12 janvier 2016, n° 37138/14, § 25 ; *Boaca et al. c. Roumanie*, 12 janvier 2016, § 35 ; *Grigoryan et Sergeyeva c. Ukraine*, 28 mars 2017, n° 63409/11, §§ 40 et 97 ; *Aycaguer c. France*, 22 juin 2017, n° 8806/12, §§ 3, 11, 14, 17, 27, 35 et 46 ; *Barbulescu c. Roumanie* [GC], 5 septembre 2017, n° 61496/08, § 51 ; *Garib c. Pays-Bas* [GC], 6 novembre 2017, n° 43494/09, Opinion dissidente des Juges PINTO DE ALBUQUERQUE et VEHABOVIC, § 29 ; *Ivashchenko c. Russie*, 13 février 2018, n° 61064/10, § 83 ; *Kurt c. Autriche*, 4 juillet 2019, n° 62903/15, § 57 ; *Pryanishnikov c. Russie*, 10 septembre 2019, n° 25047/05, Opinion concordante du Juge PINTO DE ALBUQUERQUE, § 14 ; *T.K. et S.R. c. Russie*, 19 novembre 2019, n° 28492/15 et 49975/15, § 44 ;

de ces arrêts, la Cour EDH s'est penchée sur une possible violation de l'art. 8 CEDH[163]. Toutefois, comme nous l'avons vu plus haut déjà, il est concevable que le profilage porte atteinte à d'autres droits fondamentaux consacrés dans la CEDH. Ainsi, dans plusieurs affaires, la notion de profilage est citée dans le cadre d'une éventuelle violation des art. 3 CEDH (interdiction de la torture)[164], 6 al. 1er CEDH (droit à un procès équitable)[165], 10 CEDH (liberté d'expression)[166], 14 CEDH (interdiction de discrimination)[167], art. 2 al. 1er du Protocole 4 (liberté de circulation sur le territoire d'un État)[168]. De plus, force est de constater que la plus ancienne de ces affaires date de 2008, la plus récente de septembre 2022, ce qui constitue un indice que l'utilisation de cette notion est nouvelle et que très peu unifiée. La majorité des affaires citées renvoyaient à des litiges nés dans le contexte de contrôles d'identité, voire d'arrestations jugées racistes (racial profiling ; ethnic profiling)[169], d'autres renvoyaient au profilage ADN[170], d'autres

N.D. et N.T. c. Espagne [GC], 13 février 2020, n° 8675/15 et 8697/15, § 163 ; *Khan c. Danemark*, 12 janvier 2021, n° 26957/19, § 34 ; *Terna c. Italie*, 13 janvier 2021, n° 21052/18, § 82 ; *Big Brother Watch et al. c. Royaume-Uni* [GC], 25 mai 2021, n° 58170/13, 62322/14 et 24960/15, Opinion en partie concordante et en partie dissidente du Juge PINTO DE ALBUQUERQUE, § 22 ; *Ekimdzhiev et al. c. Bulgarie*, 11 janvier 2022, n° 70078/12, § 364 ; *Khasanov et Rakhmanov c. Russie* [GC], 29 avril 2022, n° 28492/15 et 49975/15, §§ 59, 79, 123 et 132 ; *Rabczewska c. Pologne*, 15 septembre 2022, n° 8257/13, §§ 24 et 26. On notera que j'ai procédé à deux simples recherches (l'une en français et l'autre en anglais) sur la plateforme « HUDOC », voir https://hudoc.echr.coe.int.

163 À titre d'exemple, *S. et Marper c. Royaume-Uni* [GC], 4 décembre 2008, n° 30562/04 et 30566/04 ; *Dubetska et al. c. Ukraine*, 10 février 2011, n° 30499/03 ; *Barbulescu c. Roumanie* [GC], 5 septembre 2017, n° 61496/08 ; *Big Brother Watch et al. c. Royaume-Uni* [GC], 25 mai 2021, n° 58170/13, 62322/14 et 24960/15, Opinion en partie concordante et en partie dissidente du Juge PINTO DE ALBUQUERQUE ; *Ekimdzhiev et al. c. Bulgarie*, 11 janvier 2022, n° 70078/12.

164 À titre d'exemple, *Vladimir Vasilyev c. Russie*, 10 janvier 2012, n° 28370/05.

165 À titre d'exemple, *Vladimir Vasilyev c. Russie*, 10 janvier 2012, n° 28370/05.

166 À titre d'exemple, *Fáber c. Hongrie*, 24 juillet 2012, n° 40721/08, Opinion dissidente de la Juge KELLER ; *Big Brother Watch et al. c. Royaume-Uni* [GC], 25 mai 2021, n° 58170/13, 62322/14 et 24960/15, Opinion en partie concordante et en partie dissidente du Juge PINTO DE ALBUQUERQUE ; *Rabczewska c. Pologne*, 15 septembre 2022, n° 8257/13, §§ 24 et 26.

167 À titre d'exemple, *Ciorcan et al. c. Roumanie*, 27 janvier 2015, n° 29414/09 et 44841/09. Il convient de noter que l'art. 14 CEDH ne peut pas être invoqué à lui seul. En d'autres termes, une discrimination ne peut se faire valoir qu'en conjonction avec la violation d'un autre droit fondamental consacré par la CEDH.

168 À titre d'exemple, *Garib c. Pays-Bas* [GC], 6 novembre 2017, n° 43494/09, Opinion dissidente des Juges PINTO DE ALBUQUERQUE et VEHABOVIC.

169 À titre d'exemple, *Dembele c. Suisse*, 24 septembre 2013, n° 74010/11 ; *Terna c. Italie*, 13 janvier 2021, n° 21052/18 ; *Khasanov et Rakhmanov c. Russie* [GC], 29 avril 2022, n° 28492/15 et 49975/15, §§ 59, 79, 123 et 132.

170 À titre d'exemple, *Aycaguer c. France*, 22 juin 2017, n° 8806/12.

encore mentionnaient le profilage dans le cadre du diabète du requérant[171], une seule de ces affaires concernait un litige né dans le contexte d'une relation de travail de droit privé[172]. Dans aucune de ces affaires citées, la Cour EDH n'en vient à définir la notion. Pour l'heure, elle n'a donc pas encore été amenée à déterminer le cadre qu'elle souhaite (éventuellement) donner au profilage en Europe[173]. La notion n'apparaît pas non plus dans une des fiches thématiques pertinentes dans le cadre de cette contribution[174].

Cela étant, d'autres organes du Conseil de l'Europe ont joué un rôle précurseur en matière de protection des données au niveau mondial ou ont offert un forum à d'importantes négociations en la matière, notamment à celles menées par les États membres qui ont conduit à l'adoption de la Convention 108 le 28 janvier 1981.

b. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après «Convention 108») du Conseil de l'Europe a été adoptée, par les États membres du Conseil de l'Europe, au début des années 1980 dans le but d'étendre le droit au respect de la vie privée des citoyens européens en prenant en compte l'augmentation des flux, nationaux et internationaux, de données personnelles au travers de traitements automatisés[175]. Il s'agit du premier instrument international contraignant au monde dans le domaine de la protection des données[176]. L'UE elle-même souhaite y adhérer, le Rapporteur spécial de l'ONU conseille la ratification à tous les États membres de l'ONU[177]. La Suisse quant à elle l'a ratifiée le 2 octobre 1997.

171 *Vladimir Vasilyev c. Russie*, 10 janvier 2012, n° 28370/05.

172 Dans l'affaire *Barbulescu c. Roumanie* [GC], 5 septembre 2017, n° 61496/08 la notion de profilage n'est pas définie, mais apparaît uniquement dans une disposition du RGPD citée dans la première partie du jugement consacrée aux dispositions internationales applicables ou, du moins, à prendre en compte en tant que source d'inspiration, voir § 51 qui renvoie à l'art. 47 RGPD.

173 Pour une analyse plus approfondie de cette jurisprudence, voir *infra* Chapitre 12. Le cadre prévu par le Conseil de l'Europe.

174 Cour EDH, Unité de presse, Fiche thématique – Protection des données personnelles, septembre 2022, Cour EDH, Unité de presse, Fiche thématique – Surveillance au travail, janvier 2022 et Cour EDH, Unité de presse, Fiche thématique – Nouvelles technologies, septembre 2022. Il convient de noter que ces fiches ne lient pas la Cour, mais reflètent néanmoins quels arrêts sont importants selon la Cour EDH elle-même.

175 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Préambule.

176 EPINEY/SCHLEISS, § 3, N 23.

177 Rapporteur spécial sur le droit à la vie privée, Rapport annuel A/73/438 à l'Assemblée générale des Nations Unies, recommandation 117.e.

Contrairement à la CEDH, la Convention 108 est un traité international qui lie les États sans pour autant créer des droits justiciables pour les particuliers. Elle ne prévoit donc aucun mécanisme supranational qui permettrait aux personnes physiques de faire recours en cas de violation de ladite Convention. En d'autres termes, la Convention 108 n'a pas vocation à créer des droits justiciables, mais plutôt à harmoniser le niveau de protection entre les États signataires. La Convention 108 ne rend les art. 8 (et 10) CEDH pas obsolètes, mais vient, bien au contraire, complémenter la protection offerte par la CEDH[178].

Contrairement à la CEDH, la Convention 108 s'applique tant aux personnes privées qu'aux institutions publiques[179]. Même si la Convention 108 de 1981, qui est toujours en vigueur en Suisse, a joué un rôle précurseur en matière de protection des données elle ne prévoit, elle non plus, aucune définition du traitement de données connu sous le nom de « profilage » (ce qui n'a rien de surprenant vu qu'elle date de 1981).

Afin de faire face aux nouveaux développements technologiques, le Comité des Ministres a, en mai 2018, adopté un Protocole d'amendement à la Convention 108 (ci-après « Convention 108+ »). Le Protocole d'amendement est ouvert à la signature de tout État (membre du Conseil de l'Europe ou non) depuis le 10 octobre 2018. Plus d'une trentaine d'États l'ont déjà signé, entre autres la Suisse[180], et il entrera en vigueur le 11 octobre 2023, à condition qu'au moins 38 États parties soient parties au Protocole à cette date. Néanmoins, il a exercé une influence considérable sur la révision de la LPD[181].

Le nouvel art. 2 let. b de la Convention 108+ ne propose pas de définition du profilage, mais, sans utiliser ce terme, semble englober le profilage dans la nouvelle définition de « traitement de données ». En effet, cette nouvelle disposition se lit comme suit : « Le 'traitement de données' s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que (…) l'application d'opérations logiques et/ou arithmétiques à ces données ».

Même si la notion de profilage ne figure pas non plus dans le Rapport explicatif qui vient préciser la portée de l'art. 2 Convention 108+, ce dernier fixe que « le traitement de données commence par la collecte de données à caractère personnel et englobe *toutes les opérations effectuées* sur les données, qu'elles

---

178 EPINEY/SCHLEISS, § 3, N 26.

179 On notera que l'aLPD et la LPD avaient, respectivement ont cette double nature publique-privée, voir l'art. 1er LPD.

180 L'adoption de la nLPD en septembre 2020 ainsi que de l'OPDo fin août 2022 permettront à la Suisse de procéder à la ratification de la version révisée de la Convention 108 prochainement.

181 FF 2017 6589 s.

le soient *de façon totalement automatisée ou en partie seulement* »[182]. Dès lors, il semble que le Rapport explicatif vient confirmer l'affirmation selon laquelle le traitement de données connu sous le nom de profilage est couvert par la Convention 108+ (et que cette définition englobe d'autres traitements de données, en plus). Le profilage constituant un des développements technologiques majeurs non-encadrés par le droit[183], il est toutefois regrettable que les États membres du Conseil d'Europe n'aient pas réussi à se mettre d'accord sur une définition du profilage.

De manière assez surprenante, le profilage est explicitement mentionné dans le cadre des explications relatives à l'art. 9 Convention 108+. Cette disposition est consacrée aux droits des personnes dont les données personnelles ont été traitées. Ainsi, en vertu de l'art. 9 let. c « les personnes concernées ont le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données, y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage »[184]. En d'autres termes, et contrairement à ce qui a pu être décidé au sein de l'UE[185], le profilage n'a pas été défini par les États membres du Conseil de l'Europe lors de l'adoption du Protocole d'amendement. Cependant, les risques liés à l'utilisation de ce traitement de données ont été reconnus dans la mesure où le profilage est mentionné dans le cadre des précisions relatives aux moyens de recours renforcés qui devraient être mis à disposition des personnes concernées. Contrairement à ce qui a pu être prévu en droit suisse et en droit de l'UE, il découle de ces explications qu'en vertu de la Convention 108+, le profilage n'est toutefois pas considéré, d'un point de vue conceptuel, comme traitement de données à lui seul. Cette combinaison de deux traitements de données distincts

182 Rapport explicatif relatif à la Convention 108+, pt. 21 ; italique ajouté par mes soins.

183 BÜCHI et al., p. 16 ; pour des précisions allant dans le même sens par rapport à l'adoption compliquée du RGPD, voir CHRISTL/SPIEKERMANN, p. 139 ; pour une illustration des difficultés américaines dans ce contexte, FRENKEL et KANG précisent à propos du réseau social *Facebook*, qui est en mesure d'effectuer des profilages de ses utilisateurs sur la base de 50'000 catégories différentes, qu'« [traduction] il était plus difficile d'obtenir l'autorisation du gouvernement pour une licence radio dans la région rurale du Montana ou de lancer un nouveau jouet pour enfants que d'établir un réseau social pour un quart de l'humanité. Au cours des deux dernières décennies, le Congrès a proposé de nombreux projets de loi sur la protection des données en ligne, mais ils sont tous tombés à l'eau en raison de la pression énorme exercée par les lobbyistes des entreprises de technologie sur les détails de ces projets de loi et de l'impasse politique au Congrès », voir FRENKEL/KANG, p. 198.

184 Rapport explicatif relatif à la Convention 108+, pt. 77.

185 Voir *infra*, Chapitre 2. La définition compliquée du profilage.

(profilage et décision automatisée) renvoie, à tout le moins, d'un point de vue du respect des droits fondamentaux, aux utilisations du profilage les plus problématiques[186].

c. La Recommandation CM/Rec(2021)8 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

Le Comité des Ministres – institution chargée d'assurer la représentation nationale des États membres au sein du Conseil de l'Europe – peut adopter des recommandations (non-contraignantes) à l'intention des États membres[187]. Persuadé qu'il était nécessaire, afin de sauvegarder les libertés et droits fondamentaux des individus, de réglementer le profilage en termes de protection des données à caractère personnel, le Comité des Ministres a adopté la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (ci-après « Recommandation profilage 2010 ») le 23 novembre 2010 déjà[188]. Constatant que les méthodes et l'impact du profilage ont radicalement changé depuis[189], il a adapté cette Recommandation aux développements technologiques des dernières années et a publié une Recommandation révisée en novembre 2021[190] (ci-après « Recommandation profilage 2021 »). Même s'il est vrai que les Recommandations du Comité des Ministres n'ont pas valeur contraignante, la Cour EDH y recourt fréquemment lorsqu'elle est amenée à apporter une solution à un problème nouveau[191]. C'est la raison pour laquelle il convient de se pencher sur la

186 Art. 2.10 Recommandation profilage 2021 ; pour une liste d'exemples particulièrement problématiques, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 43 ss.

187 Art. 15 let. b Statut du Conseil de l'Europe.

188 Recommandation CM/Rec(2010)13 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage du 23 novembre 2010.

189 Pour un aperçu plus détaillé des développements intervenus depuis l'adoption de la Recommandation profilage 2010, voir Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Report on Developments after the Adoption of Recommandation (2010)13 on Profiling, pp. 6 ss.

190 Recommandation CM/Rec(2021)8 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage du 3 novembre 2021.

191 À titre d'exemple, voir *Barbulescu c. Roumanie* [GC], 5 septembre 2017, n° 61496/08, §§ 43 et 138 ou *López Ribalda et al. c. Espagne* [GC], 17 octobre 2019, n° 1874/13 et 8567/13, § 62. Dans ces deux affaires, la Cour EDH s'appuie non pas sur la Recommandation CM/Rec(2010)13 mais sur la Recommandation CM/Rec(2015)5 sur le traitement des données à caractère personnel dans le cadre de l'emploi du 1er avril 2015.

définition du profilage proposée par le Comité des Ministres. De plus, on rappellera qu'il s'agit de la seule définition à proprement parler adoptée par un organe du Conseil de l'Europe.

La définition révisée du profilage est désormais consacrée à l'art. 1er let. c Recommandation profilage 2021 qui se lit comme suit : « [le] profilage désigne toute forme de traitement automatisé de données à caractère personnel, notamment au moyen de systèmes d'apprentissage automatique, consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne »[192]. En d'autres termes, pour le Comité des Ministres, le profilage se caractérise par les trois éléments cumulatifs suivants :

— toute forme de traitement automatisé ;
— de données à caractère personnel ;
— dans le but d'évaluer certains aspects personnels relatifs à une personne physique.

Longtemps considéré une anomalie du régime juridique suisse, le profilage à risque élevé a fait son entrée dans la Recommandation profilage 2021. Ainsi, l'art. 1er let. j se lit comme suit : « 'traitements de profilage à risque élevé' peut notamment désigner :

— le profilage dont le fonctionnement entraîne des effets juridiques ou qui ont un impact significatif pour la personne concernée ou pour le groupe de personnes identifié par le traitement de profilage ;
— le profilage qui – en raison du public visé, du contexte ou de la finalité du traitement – en particulier dans une situation de déséquilibre dans le pouvoir d'information, comporte un risque d'affecter ou d'influencer indûment les personnes concernées, notamment lorsqu'il s'agit de mineurs ou d'autres personnes vulnérables ;
— le profilage implique des données relevant des catégories particulières de données au sens de l'article 6 de la Convention 108+ ou ayant pour finalité de les détecter ou les prédire ;
— le profilage affectant un très grand nombre de personnes, notamment celui opéré par des services d'intermédiaires en ligne pour leur bénéfice propre ou pour celui de tiers ».

192 On rappellera que la définition prévue à l'art. 1er let. e Recommandation profilage 2010 fixait que le profilage était : « une technique de traitement automatisé des données qui consiste à appliquer un 'profil' à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels ».

Si le Conseil de l'Europe a le mérite d'avoir été la première institution à proposer une définition du profilage, elle n'est pas la seule à s'être interrogée pour définir cette nouvelle forme de traitement. En effet, l'UE en tant qu'« entité politique post-nationale *sui generis* »[193] a reconnu l'importance de légiférer de manière contraignante en matière de profilage grâce à un instrument légal qui prévoit des droits directement invocables par les citoyens européens : le Règlement général sur la protection des données du 27 avril 2016[194]. De plus, comme il a déjà été mentionné plus haut, ce Règlement a une portée extraterritoriale[195], qui n'est toutefois sans importance dans le cadre de cette contribution[196]. En outre, on rappellera que le Législateur suisse s'en est inspiré lorsqu'il a révisé la LPD[197]. Il convient dès lors de se pencher sur la définition du profilage adoptée par l'UE.

3. La définition en droit européen

Le Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données du 27 avril 2016 (ci-après « RGPD »), en vigueur depuis le 25 mai 2018, est la première législation contraignante au niveau mondial directement invocable par les personnes concernées, qui définit le traitement de données connu sous le nom de « profilage ». Ainsi, l'art. 4 ch. 4 RGPD définit le profilage comme étant « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ». La liste des buts recherchés lors de l'utilisation du profilage est non-exhaustive[198].

193 Notion reprise de BESSON, voir BESSON, Droit constitutionnel européen, N 172.

194 Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit Règlement général sur la protection des données.

195 Art. 3 RGPD.

196 Si DAEDELOW est d'avis qu'une application extraterritoriale est concevable, entre autres lorsqu'un employeur suisse recrute un candidat qui se trouve dans l'UE, cet exemple d'application extraterritoriale du RGPD n'est pas pertinent, voir DAEDELOW, p. 37 et MÉTILLE/ACKERMANN, pp. 82 ss. respectivement ; pour une explication plus précise de la portée de cette disposition en droit suisse, voir *supra* Méthodologie.

197 ROSENTHAL, Das neue Datenschutzgesetz, N 2 et 9.

198 HELFRICH, art. 4 ch. 4 RGPD, N 84.

En de termes plus simples, le profilage, en droit européen, s'entend des trois éléments cumulatifs suivants :
- toute forme de traitement automatisé ;
- de données à caractère personnel ;
- dont le but est d'évaluer certains aspects personnels relatifs à une personne physique (afin d'influencer les interactions avec la personne concernée)[199].

Dans le cadre de cette sous-section, il est intéressant de relever que la définition ressemble à celle fixée à l'art. 5 let. f LPD ce qui n'a rien de surprenant étant donné que le Législateur suisse s'est inspiré des travaux de l'UE en la matière[200]. De plus, l'UE a décidé de mentionner la relation de travail comme la première relation juridique potentiellement affectée par un usage excessif du profilage – avant même de mentionner le secteur du crédit[201], qui a pourtant vu naître le profilage[202].

Les définitions proposées et par le Conseil de l'Europe et par l'UE ainsi que celle adoptée par le Parlement suisse se rejoignent sur quelques points, mais se distinguent sur d'autres points. Dans la mesure où ces trois définitions pourraient toutes trouver à s'appliquer en Suisse, il convient de brièvement les comparer.

4. Comparaison des différentes définitions

À titre préliminaire, on notera que la révision de la Recommandation profilage 2010 a conduit à un alignement de la définition du profilage proposée par le Comité des Ministres sur celles qui sont en vigueur en droit suisse et en droit de l'UE.

Si cette convergence des trois définitions du profilage potentiellement applicables en Suisse est à saluer, notamment au nom de la sécurité juridique, il est regrettable que dans le cadre de cette révision, le Comité des Ministres ait introduit une nouvelle spécificité propre à la Recommandation profilage 2021. En effet, il a introduit la notion de « profilage à risque élevé », qui était considérée

199 KLABUNDE, art. 4 RGPD, N 28 ; utilisant un vocabulaire légèrement distinct, le Groupe « Article 29 » précise que le but du profilage consiste à appliquer la corrélation à une personne pour déduire les caractéristiques du comportement actuel ou futur d'une personne, voir Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 8.

200 FF 2017 6641.

201 Dans le secteur du crédit, la pratique du profilage est souvent désignée sous le nom de « scoring », voir HELFRICH, art. 4 ch. 4 RGPD, N 87 s. ou Exposé des motifs relatif à la Recommandation profilage 2010, pt. 43.

202 O'NEIL, pp. 141 ss.

jusqu'alors une anomalie du droit suisse. Toutefois, il propose une tout autre définition de cette forme de traitement de données que celle qui a été consacrée par le Législateur suisse. Si la définition du profilage à risque élevé telle que proposée par le Comité des Ministres est plus complète que celle prévue en droit suisse, le profilage à risque élevé tel qu'entendu par le Comité des Ministres correspond au traitement de données connu sous le nom de « décision individuelle automatisée » en droit suisse. La confusion est totale. Ainsi, on constatera que le Comité des Ministres ne procède toujours pas à une distinction claire entre un profilage et une décision individuelle automatisée[203].

Parmi les nouvelles définitions proposées par le Comité des Ministres, ce dernier définit les « systèmes automatisés de prise de décision ». Cette notion est inconnue tant en droit suisse qu'en droit de l'UE. Reste à savoir ce qui devra être entendu par ce traitement de données en pratique et dans quelle mesure il se distingue du profilage à risque élevé tel qu'entendu par le Comité des Ministres.

Enfin, on retiendra que la définition du profilage à risque élevé en droit du Conseil de l'Europe est légèrement plus large que celle connue en droit suisse. D'une part, elle englobe également les profilages de groupe alors que la définition suisse ne porte que sur des évaluations individuelles. Reste à connaître l'impact de cette définition plus large en pratique. Dans le cadre de cette contribution, cette question est sans importance dans la mesure où le profilage d'un candidat est un profilage individuel. D'autre part, la troisième hypothèse d'un profilage à risque élevé telle que proposée par le Comité des Ministres semble traduire une approche plus dynamique à la notion de donnée sensible (ce qui

203 On rappellera qu'en vertu du droit suisse, le profilage a pour but d'évaluer certains aspects (essentiels et non-essentiels) relatifs à une personne physique alors que la Recommandation profilage 2010 prévoyait que le profilage pouvait servir deux buts distincts, c'est-à-dire *soit* une prise de décision juridique *soit* une analyse, voire une prédiction des préférences, comportements ou attitudes d'une personne physique. En d'autres termes, la Recommandation profilage 2010 excluait de son champ d'application les traitements qui ne comprenaient pas d'inférences (voir Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 7). Le droit de l'UE quant à lui prévoit que le but recherché d'un profilage consiste à évaluer certains aspects personnels d'une personne physique sans toutefois préciser s'il s'agit d'aspects essentiels ou non-essentiels (Le Groupe « Article 29 » précise que le but du profilage consiste à appliquer la corrélation à une personne pour déduire les caractéristiques du comportement actuel ou futur, voir Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 8). Ainsi, afin de tomber sous la définition du droit de l'UE ou celle prévue en droit suisse, il n'est pas nécessaire que le traitement de données ait nécessairement pour but d'influencer une interaction avec la personne concernée (même si tel sera souvent le cas), mais qu'une évaluation de certains traits de la personnalité soit envisagée, c'est-à-dire que les données personnelles soient soumises à un procédé de nature subjective.

est à saluer). De plus, il semblerait qu'un profilage effectué à grande échelle dans le seul but de faire du profit constitue un profilage à risque élevé ce qui ne devrait pas correspondre à la position du Législateur suisse. Estimant que la grande majorité des courtiers en données effectuent des profilages à grande échelle dans le but de faire du profit, reste à savoir dans quelles hypothèses les profilages effectués ne constituent *pas* des profilages à risque élevé en vertu de la Recommandation profilage 2021. En d'autres termes, le risque élevé d'un profilage devrait être plus souvent admis à la lumière de la Recommandation profilage 2021 qu'à la lumière de la définition suisse.

Cette comparaison peut également être résumée grâce au tableau suivant :

Figure 2 : Comparaison des différentes définitions du « profilage » potentiellement applicables en Suisse

	Entrée en vigueur	**Traitements couverts**	**Catégories de données**	**Buts recherchés**	**Lien avec la décision individuelle automatisée**
Suisse	2023	Traitement entièrement automatisé	Données personnelles	Évaluation de certains aspects de la personnalité	Combinaison possible
		Sous-catégorie du « profilage à risque élevé » (déf. vague)			
Conseil de l'Europe	2010, déf. révisée en 2021	Traitement automatisé	Données personnelles	Évaluation de certains aspects de la personnalité	Délimitation peu claire entre le profilage à risque élevé et la décision individuelle automatisée
		Sous-catégorie du « profilage à risque élevé » (liste non-exhaustive de 4 ex. ; depuis 2021)			
Union européenne	2018	Traitement entièrement ou partiellement automatisé	Données personnelles	Évaluation de certains aspects de la personnalité	Combinaison possible

Afin de mieux comprendre les enjeux du profilage, il convient de dresser un bref aperçu (non-exhaustif) des différentes utilisations qui peuvent en être faites.

Chapitre 3. Exemples de profilage dans différents secteurs d'activités

D'abord, et c'est ce contexte qui nous intéressera par la suite, il peut s'avérer avantageux, pour un employeur, de recourir au profilage aux différents stades d'une relation de travail, notamment lors de la procédure d'embauche lorsqu'il s'agit de choisir le « meilleur » candidat, pendant la relation de travail lorsqu'il s'agit de déterminer quels employés sont particulièrement performants et méritent, p. ex., une hausse de salaire ou, enfin, lorsque dans un contexte de fusions, il s'agit de déterminer quels employés devraient être licenciés dans le but de garder les employés les plus efficaces[204]. Ainsi, le profilage peut être utilisé pour analyser les mots utilisés dans les courriels électroniques, le ton de la voix lorsque l'employé concerné répond à ses collègues ou aux clients ou encore la vitesse à laquelle l'employé en question frappe sur son clavier. Ces différentes analyses peuvent permettre de déterminer, entre autres, l'esprit d'équipe d'une personne concernée[205].

Ensuite, et cela est pratique courante depuis de nombreuses années, les instituts de crédit recherchent à savoir si un client potentiel remboursera ou non son crédit à temps. À cette fin, les instituts de crédit eux-mêmes ou alors des tiers spécialisés dans cette forme de traitements de données[206] vont, à titre d'exemple, évaluer grâce à des algorithmes « performants » la vitesse à laquelle les factures sont payées, la fréquence à laquelle la limite de crédit est dépassée

204 O'NEIL, p. 132 ; KASPER/WILDHABER, Big Data am Arbeitsplatz, pp. 224 ss. ; MORGENROTH, p. 156.

205 Pour une analyse approfondie des différentes techniques d'analyse de données (personnelles ou pas) qui sont utilisées aux différents stades d'une relation de travail, voir KASPER/WILDHABER, Big Data am Arbeitsplatz, pp. 194 ss. ; pour un aperçu et une brève analyse juridique des différentes nouvelles formes de traitements de données *pendant* la relation de travail (*wearables*, traitements de données biométriques, vidéosurveillance etc.), voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, pp. 63 ss. Les auteurs abordent également les nouveaux défis engendrés par l'avènement généralisé du télétravail, voir idem, pp. 79 ss. ; au sujet de la surveillance mise en place suite à l'avènement du télétravail, on consultera également l'étude menée entre juillet et août 2021 dans plus de 20 pays, qui a dévoilé à quel point il sera délicat pour les employeurs de trouver le bon équilibre entre les différents intérêts en cause lorsqu'ils souhaitent évaluer les performances de leurs employés à distance, voir vmware, The Virtual Floorplan, New Rules for a New Era of Work.

206 À titre d'exemple, voir l'arrêt du Tribunal administratif fédéral du 18 avril 2017 (A-4232/2015) *Moneyhouse*, qui a été rendu après une procédure d'établissement des faits en vertu de l'art. 29 aLPD engagée par le PFPDT en tant qu'autorité de surveillance.

ou le quartier dans lequel le potentiel débiteur réside. Sur la base de ces évaluations, les instituts de crédit vont déterminer s'il est judicieux d'octroyer un crédit à la personne concernée et si oui, sous quelles conditions[207].

Après, et dans une veine similaire, les assurances ont, de plus en plus, elles aussi, tendance à recourir au profilage lorsqu'il s'agit de déterminer les primes d'assurance. Dans ce contexte, il est connu de longue date que les assureurs effectuent un profilage non seulement lorsqu'il s'agit de déterminer le montant d'une prime[208], mais aussi lorsqu'il s'agit de déterminer quel client mérite d'être servi en premier par le service aux clients[209]. Si les assureurs suisses ne semblent pas (encore) procéder à l'individualisation des conditions contractuelles, ils tentent de plus en plus d'aller dans cette direction et, ce faisant, remettent en question le principe de solidarité qui sous-tend le secteur de l'assurance[210].

Dans le secteur privé, on notera que le profilage peut également être effectué dans le cadre de la recherche médicale, notamment afin de détecter des maladies génétiques[211], ou encore dans le domaine commercial dans la mesure où le profilage permet d'adapter le prix d'un bien ou d'un service en fonction du profil du consommateur[212].

Par ailleurs, les activités du secteur public n'échappent pas au profilage. À titre d'exemple, un profilage a pu déterminer quels citoyens avaient le droit à une prestation publique[213] ou lesquels étaient susceptibles d'éluder l'impôt de manière frauduleuse[214].

207 HEUBERGER, N 159 ss. ; O'NEIL, pp. 141 ss. ; Exposé des motifs relatif à la Recommandation profilage 2010, pt. 43.

208 HEUBERGER, N 166 ; Arrêt du Tribunal administratif fédéral du 19 mars 2019 (A_3548/2018) *Helsana+*.

209 WALTER, Le profilage, pp. 88 s.

210 Pour une analyse critique de ces développements dans le secteur des assurances, voir ZITTEL/FUHRER, pp. 71 ss., MEIER, Big Data, p. 94 et ROUVROY, pp. 15 s. ; pour une analyse plus souple du cadre légal, voir THOUVENIN, Individualisierung, pp. 21 ss. ; pour une analyse en quatre temps des nouvelles formes de traitements de données dans le domaine de la santé et leurs effets potentiels sur le principe de solidarité et le rôle de l'État, voir SAMOCHOWIEC/MÜLLER, pp. 5 ss.

211 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 44.

212 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 46.

213 Pour un aperçu de profilages effectués par différentes autorités à travers l'Europe, voir AlgorithmWatch, Stories ; pour plusieurs exemples américains, on consultera le résumé des recherches menées par EUBANKS, qui précise, à juste titre, que les profilages actuellement mis en place par les pouvoirs publics américains affectent avant tout les populations pauvres. Toutefois, elle estime que ces mesures de surveillance, une fois mises en place, finiront par être appliquées à la totalité de la population, voir EUBANKS, pp. 1 ss. et spécifiquement p. 12.

214 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 45 ; pour un résumé de l'intervention récente du PFPDT par rapport au projet de l'OFS relatif à une modification

De plus, il est toujours difficile d'estimer le risque de récidive d'une personne incarcérée. Ainsi, il est possible d'effectuer un profilage afin d'évaluer le comportement de la personne concernée et de procéder à une prédiction automatisée de la probabilité d'une récidive[215]. Un profilage peut également être effectué avant même que la personne concernée ne passe à l'acte[216]. Dès lors, un juge indécis quant à la peine à prononcer ou quant à la liberté conditionnelle à octroyer pourrait être tenté de recourir au profilage afin de laisser cette forme de traitement automatisé influer sur sa décision.

En outre, toute contribution au sujet du profilage serait incomplète si elle ne mentionnait pas les mesures de surveillance mises en place dans le cadre de la lutte contre le terrorisme. Ces mesures ont pour but d'identifier les terroristes avant qu'ils ne passent à l'acte, notamment sur la base de profilages effectués à (très) grande échelle. En comparant des données collectées à des comportements particuliers considérés comme suspects, le forage de ces données permet d'établir des profils d'individus suspects. Ainsi, ce traitement de données risque d'aboutir à ce que des innocents deviennent suspects sur la base de profils erronés[217].

Enfin, on rappellera que l'entreprise britannique *Cambridge Analytica*, qui a fait la une de la presse mondiale en 2018, a elle aussi eu recours au profilage tel que défini en droit suisse. Sur la base de données personnelles dérobées à *Facebook*, *Cambridge Analytica* a créé un logiciel permettant d'agréer ces données personnelles à d'autres données d'intérêt électoral. Cette agrégation de

de l'ordonnance sur les relevés statistiques qui prévoyait un nouveau relevé de données fiscales, notamment en raison d'un danger de profilage, voir PFPDT, 29e Rapport d'activités, pp. 16 s.

215 O'NEIL, pp. 24 ss. ; pour un exemple catalan, voir AlgorithmWatch, In Catalonia the Ris-Canvi Algorithm Helps Decide Whether Inmates Are Paroled.

216 GROSSENBACHER, « Predictive Policing », Polizei-Software verdächtigt zwei von drei Personen falsch ; pour une analyse critique de cette évaluation policière qui a malencontreusement été qualifiée de « *predictive policing* » par la presse, voir LOEWE-BAUR, pp. 153 ss. ; En effet, il convient de distinguer cette forme de profilage des méthodes d'analyse opérationnelle (également connues sous le nom anglais de « *predictive policing* »), qui se fondent aussi sur des évaluations automatisées de données, mais qui n'ont pas pour but d'utiliser l'information obtenue pour des décisions relatives à une personne déterminée, mais d'établir un phénomène général sur une population. Dès lors, bien que ces mesures puissent avoir des conséquences problématiques pour des individus, elles ne tombent pas sous la définition de profilage telle que prévue en droit suisse. En 2010 déjà, le Comité des Ministres excluait ces traitements de données du champ de la Recommandation profilage 2010, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 42 et, pour plusieurs exemples américains, voir O'NEIL, pp. 84 ss.

217 WALTER, Le profilage, p. 91 ; dans une veine plus critique (plusieurs années avant les révélations SNOWDEN) et avec de plus amples détails quant aux mesures de surveillance mises en œuvre, voir MEIER, Protection des données, N 320 et Exposé des motifs relatif à la Recommandation profilage 2010, pt. 54.

données a ensuite permis à cette entreprise britannique de psychologiquement manipuler les électeurs en leur envoyant des publicités ciblées, notamment en fonction de leur profil psychologique créé sur la base des données dérobées au réseau social[218].

Les quelques exemples susmentionnés ne reflètent en aucun cas toutes les utilisations possibles du profilage. Le potentiel de cette nouvelle forme de traitement de données reste à être déterminé. Ces quelques exemples illustrent cependant qu'il peut être envisagé de recourir au profilage dans des situations très diverses, le plus souvent à l'insu de la personne concernée : dans le secteur public ou privé, au stade précontractuel d'une relation contractuelle, pendant une relation contractuelle ou alors à la fin d'une telle relation. Les listes non-exhaustives figurant aux art. 5 let. f LPD et 4 ch. 4 RGPD reflètent cet état de fait.

Malgré des utilisations très diverses du profilage, les relations juridiques potentiellement affectées par le profilage sont, en principe, des relations asymétriques[219]. Le profilage n'est, en principe, pas utilisé réciproquement. En d'autres termes, la partie contractuelle, voire l'institution publique qui effectue un profilage se trouve souvent dans une position de pouvoir – ne serait-ce que parce que grâce au profilage elle détient plus d'information par rapport à son cocontractant que la personne dont les données personnelles sont traitées[220]. C'est entre autres pour cette raison que toutes les constellations susmention-

218 Pour un résumé détaillé du scandale qui éclata en 2018, voir FRENKEL/KANG, pp. 182 ss. et pour un aperçu de la stratégie poursuivie lors de la deuxième campagne présidentielle de TRUMP en 2020, voir idem, pp. 290 s. ; pour le témoignage de DEHAYE devant la commission compétente de la Chambre des communes du Royaume-Uni, voir House of Commons, Digital, Culture, Media and Sport Committee, Oral evidence : Fake News, HC 363, 27 mars 2018, questions 1388 ss., <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81022.html> (dernière consul-tation le 14 mars 2022) ; on notera que le Comité des Ministres relevait, en 2010 déjà, que le profilage pourrait être utilisé à des fins politiques dans la mesure où un parti politique, une association ou un groupe d'activités pourrait s'en servir afin de profiler de manière très fine chacun des électeurs et, éventuellement, adapter en temps réel la présentation électronique de son programme politique en fonction d'un profil donné. Dans la même veine, il indique que le profilage pourrait être mis en place sur les réseaux sociaux afin de détecter les individus les plus rebelles, les discriminer ou les écarter, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 35 ; pour une analyse approfondie du cadre constitutionnel et pénal suisse d'une telle manipulation, voir LUBISHTANI/FLATTET, pp. 710 ss. ; le PFPDT ayant reconnu le risque lié à l'utilisation des réseaux sociaux dans le cadre d'une campagne électorale a publié, en collaboration avec les préposés cantonaux de la protection des données (privatim), un « Guide relatif aux élections et votations » le 6 juin 2019, voir PFPDT, Guide relatif aux élections et votations.

219 MORGENROTH, p. 107 ; CUSTERS/URSIC, p. 339 ; ROUVROY, p. 19 ; spécifiquement à propos de *Facebook*, voir FRENKEL/KANG, pp. 323 s.

220 Dans le même sens, voir la définition du profilage à risque élevé telle que proposée par le Comité des Ministres à l'art. 1er let. j Recommandation profilage 2021.

nées ont comme point commun que le recours à cette nouvelle forme de traitement de données soulève d'importantes questions relatives au respect des droits fondamentaux. En effet, il est facilement concevable que la partie dominante à la relation juridique abuse de sa position et par-là porte atteinte à la personnalité, voire à un intérêt protégé par les droits fondamentaux de la personne concernée par le profilage[221]. Toutefois, dans un souci de brièveté, cette contribution se concentrera sur le profilage dans le cadre de la procédure d'embauche, qui constitue un exemple parmi d'autres de traitements de données communément regroupés sous la notion de « People Analytics »[222].

Chapitre 4.
People Analytics : le profilage sur le lieu de travail

Afin de mener les développements juridiques à bon port, il convient de brièvement circonscrire la notion de « People Analytics » (A) avant de présenter les différentes possibilités d'utilisation de cette forme de profilage, notamment dans le cadre d'une procédure d'embauche (B).

A. Définition(s)

« HR Analytics », « Workforce Analytics », « Talent Analytics », « Human Capital Analytics », « Workplace Analytics », « Human Ressource Intelligence », « New Control », « Performance Management », « Workforce Science », « Workplace Surveillance », « Pre-Employment-Check », « People Analytics ». Toutes ces différentes notions désignent des traitements automatisés de données personnelles de candidats, voire d'employés. S'agissant d'un phénomène nouveau, il n'existe pas (encore) une notion unique pour qualifier ces traitements de données[223].

221 « [traduction] La supériorité des entreprises s'oppose à la vulnérabilité de leurs clients. Dans la terminologie traditionnelle des droits fondamentaux, les clients sont atteints dans leur 'qualité de sujet' lorsque leur acceptation sociale est remise en question de manière quasi arbitraire par les entreprises en raison des traitements de données », voir MORGENROTH, p. 33 qui cite, dans la deuxième partie de ce passage, THOMAS PETRI, Préposé bavarois à la protection des données depuis 2009.

222 On traduira cette notion par « analyse de données liées au personnel ». Pour des raisons de lisibilité toutefois et en raison du fait que le terme anglais est également fréquemment utilisé dans la littérature francophone, le terme anglais sera utilisé tout au long de la contribution.

223 Cette liste est reprise de la contribution de KASPER et WILDHABER, voir KASPER/WILDHABER, Big Data am Arbeitsplatz, p. 191 ; dans leur rapport publié en 2021, KAUFMANN et SCHUERCH quant à eux mentionnent les notions de «Hiring by Algorithms», «E-Recruting»

Même s'il est vrai que la LPD mentionne l'analyse ou la prédiction des éléments concernant le rendement au travail comme un des buts possibles du profilage et que le nombre d'entreprises suisses ayant recours au profilage semble augmenter d'année en année[224], il n'existe, au niveau suisse, aucune définition légale de la notion de « People Analytics ». Le Tribunal fédéral n'a quant à lui pas (encore) été amené à se prononcer par rapport à cette notion et à ses éventuels contours.

Au niveau international, l'art. 4 ch. 4 RGPD prévoit que le profilage dans le contexte du travail doit être entendu comme une technique permettant d'« analyser ou prédire des éléments concernant le rendement au travail ». En d'autres termes, le RGPD ne définit pas la notion précise de « People Analytics », mais mentionne, en premier (comme la LPD), parmi les relations juridiques potentiellement concernées par le profilage, la relation de travail. À ce jour, la CJUE n'a pas (encore) été amenée à définir plus précisément ce qui doit être entendu par une « analyse automatisée du rendement de travail ».

Si le Conseil de l'Europe a le mérite d'avoir proposé une définition du profilage général en 2010 déjà, il n'a pas (encore) proposé un encadrement spécifique de ce traitement de données effectué dans le cadre d'une relation de travail. Il est regrettable qu'il en aille de même de l'Organisation internationale du travail (ci-après « OIT »), qui a pourtant affirmé, dans le cadre de son centenaire en 2019, qu'elle comptait « promouvoir [...] des politiques et des mesures permettant d'assurer une protection appropriée de la vie privée et des données personnelles, de relever les défis et de saisir les opportunités dans le monde du travail qui découlent des transformations associées aux technologies numériques, notamment le travail via des plateformes »[225]. L'OCDE a également commencé à chercher à savoir dans quelle mesure l'intelligence artificielle (ci-après « IA ») allait impacter le lieu de travail. Toutefois, ses travaux en sont encore à

et de « HR Analytics » sans toutefois les définir, voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 63.

224 WILDHABER/KASPER, Quantifizierte Arbeitnehmer, p. 770 ; pour une appréciation plus réservée de ces développements, notamment dans le cadre de l'embauche, voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, pp. 59 s. et 63 ; en dehors de l'Europe, ce développement ne fait aucun doute, voir CHRISTL/SPIEKERMANN, p. 31 ; pour une liste d'exemples compilés d'entreprises offrant cette sorte de services, voir idem, pp. 31 ss.

225 On relevera que ce but est inscrit parmi bien d'autres sous le chapitre qui s'adresse aux membres de l'OIT. En d'autres termes, la protection de la vie privée des employés ne figure pas dans le chapitre précédent de la déclaration dédié aux missions de l'OIT. De plus, en vertu de la lettre, l'OIT s'inquiète avant tout de l'impact des plateformes sur le monde du travail qui fonctionnent certes également grâce à une forme de profilage, mais qui ne renvoient pas aux hypothèses qui nous intéressent dans le cadre de cette contribution, voir OIT, Déclaration du centenaire de l'OIT pour l'avenir du travail, III.C.iv.

leurs débuts et ne portent pas sur la procédure d'embauche et encore moins sur une possible définition du profilage dans le cadre d'une telle procédure[226].

À l'instar du PFPDT et de KASPER et WILDHABER, la notion la plus fréquente (et non la plus précise) sera donc utilisée tout au long des développements juridiques qui suivent : « People Analytics »[227]. Au regard de ce qui précède, il convient dès lors de s'en tenir à la définition proposée par ces deux auteurs : la notion de « People Analytics » renvoie aux nouvelles formes de gestion du personnel, qui se fondent sur une analyse algorithmique en temps réel ou à grande vitesse de quantités considérables de données des employés. Ces analyses aboutissent à des corrélations et à d'innombrables variables sur les individus[228]. Ces analyses *Big Data* aident à prendre des décisions en matière de ressources humaines (profilage) ou prennent les décisions à la place d'une personne physique (décision individuelle automatisée) – le plus souvent à la place d'un collaborateur du département des relations humaines ou d'un supérieur direct[229].

B. La mise en place de People Analytics dans le cadre d'une procédure d'embauche

À titre préliminaire, on notera que le profilage du candidat peut avoir lieu avant un éventuel entretien d'embauche (mesure de présélection), pendant l'entretien d'embauche ou à la suite d'un tel entretien (mesure venant confirmer ou infirmer le choix opéré)[230] et qu'il existe deux manières de concevoir un profilage dans le cadre d'une procédure d'embauche[231]. Chacune soulève des questions juridiques légèrement différentes.

226 OECD, Social, Employment And Migration Working Papers No. 256, The Impact Of Artificial Intelligence On The Labour Market : What Do We Know So Far ?, 25 janvier 2021 et OECD, Social, Employment And Migration Working Papers No. 265, Artificial Intelligence And Employment : New Cross-Country Evidence, 17 décembre 2021.

227 Cette notion a également été retenue par CHRISTL et SPIEKERMANN, voir CHRISTL/SPIEKERMANN p. 34 ; ce choix se justifie également dans la mesure où le concept plus général d'« Analytics and Visualization » renvoie à des services qui permettent de visualiser les résultats obtenus après une analyse de données. Ces services sont souvent offerts par des entreprises spécialisées et se distinguent d'autres services qui se fondent sur le *Big Data*, comme p. ex. Business Intelligence ou Data As A Service, pour un aperçu des différents services offerts qui se fondent sur le *Big Data*, voir BERANEK ZANON, p. 91.

228 Pour un aperçu des utilisations très variées du *People Analytics*, voir AlgorithmWatch, p. 5.

229 KASPER/WILDHABER, Big Data am Arbeitsplatz, p. 190.

230 Reatch, Wenn Künstliche [sic] Intelligenz über Bewerber*innen entscheidet, 19 octobre 2021.

231 KASPER/WILDHABER, Big Data am Arbeitsplatz, pp. 194 ss. ; dans le même sens, voir ROUVROY, p. 8.

D'une part, si l'employeur dispose des connaissances nécessaires, il peut, sur la base de données personnelles d'employés jugés efficaces, créer l'employé type (*Perfect Match*). À titre d'exemple, il pourrait s'avérer que dans l'entreprise en question, les employés les plus performants ont entre 35 et 40 ans, ont étudié dans une certaine université, résident tous à 40 km du lieu de travail au maximum, font leur pause midi entre 11 heures 45 et 12 heures 30 et sont en mesure de rédiger un courriel d'une longueur déterminée à une certaine vitesse[232]. Les données du candidat vont alors être comparées à celles du *Perfect Match*. Dans cette hypothèse on peut se demander si l'établissement d'un tel *Perfect Match* sur la base de données d'employés collectées pendant les heures de travail ne contrevient pas à l'interdiction de la surveillance du comportement sur le lieu de travail telle que consacrée à l'art. 26 Ordonnance 3 relative à la loi sur le travail[233]. À l'heure actuelle, il est peu probable que les employeurs suisses disposent des connaissances nécessaires pour créer ce *Perfect Match* et d'en tirer un avantage économique. De plus, on notera qu'il semble que certains responsables de traitement évitent de « se salir les mains » lorsqu'ils décident de mettre en place des mesures de surveillance et préfèrent recourir aux services d'un sous-traitant pour la mise en place desdites mesures, parfois sur la base de contrats oraux ou de termes contractuels vagues[234].

D'autre part, la création du *Perfect Match* peut bien évidemment être externalisée. Dans ce deuxième cas de figure, le *Perfect Match* est créé sur la base d'une analyse automatisée d'une multitude de données (potentiellement anonymes) forcément de nature plus générale que dans la première hypothèse. Ensuite, les données relatives au candidat sont comparées au *Perfect Match*.

232 Exemple inspiré de l'aperçu des différentes entreprises américaines actives dans le secteur du *People Analytics*, voir CHRISTL/SPIEKERMANN, pp. 31 ss. et CUSTERS/URSIC, p. 324 ; pour un exemple d'un tel profilage mis en place par l'assureur *AXA* dans le but de faciliter les changements de poste au sein du groupe, voir AlgorithmWatch, p. 4.

233 Ordonnance 3 relative à la loi sur le travail (OLT 3) du 18 août 1993, RS 822.113. On notera que le Commentaire de l'art. 26 OLT 3 relatif à la surveillance des travailleurs publié par le SECO reste muet à ce sujet. À juste titre, KAUFMANN et SCHUERCH précisent qu'il n'est pas toujours aisé de distinguer entre une mesure de surveillance portant sur le comportement (illicite) et une mesure visant à évaluer la performance (licite à condition qu'elle soit proportionnée), voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 65.

234 Dans son résumé de la retraite estivale du Préposé à la protection des données du *Land* du Schleswig-Holstein dédiée à la protection des données des travailleurs, HANSEN cite HERTA DÄUBLER-GMELIN, ancienne Ministre fédérale de la Justice, voir HANSEN, p. 650. Si l'article relate certes l'observation d'une politicienne allemande, la situation ne devrait pas être très différente en Suisse – d'autant plus que la Suisse connaît un régime de protection des données plus souple que l'Allemagne (ce qui était déjà le cas sous le régime de l'aLPD et de la Directive 95/46/CE remplacée par le RGPD), voir MORGENROTH, pp. 116 s.

L'évaluation de la personnalité du candidat ainsi effectuée est ensuite vendue à l'employeur. Ce sont ces hypothèses qui interpellent davantage d'un point de vue de la protection des données. En effet, l'employeur perd toute forme de contrôle sur les données qui informent l'évaluation nécessaire à la création du *Perfect Match*. Ainsi, on peut se demander comment l'employeur en tant que responsable du traitement assume ses responsabilités légales (garantie de la sécurité des données, garantie des droits d'accès etc.). De plus, il n'est pas évident de savoir si l'entreprise qui a procédé à l'évaluation du candidat doit être qualifiée de sous-traitant ou de tiers. En fonction de la réponse à cette question épineuse, le régime applicable change[235].

Étant donné que cette deuxième hypothèse domine en pratique, la présente contribution aura pour but d'examiner le cadre juridique de cette forme de profilage[236]. Toutefois, avant d'étayer ce cadre juridique, il convient de rappeler les avantages et potentiels risques juridiques liés à l'utilisation du profilage dans le cadre de procédures d'embauche.

Chapitre 5. Avantages et risques

Plusieurs avantages ainsi que plusieurs risques peuvent être identifiés lors d'un profilage effectué par un employeur. Afin de mieux cerner les enjeux du recours (non-encadré) au profilage, il convient dès lors de brièvement résumer les avantages (A) ainsi que les potentiels risques liés à l'utilisation de ce traitement de données (B).

A. Avantages

L'utilisation du profilage dans le cadre d'une procédure d'embauche offre plusieurs avantages :

D'abord, le profilage permettrait de prendre des décisions plus objectives dans la mesure où l'algorithme qui sous-tend le traitement automatisé de

235 L'art. 9 LPD règle le cas spécifique de la sous-traitance. Au contraire, la communication de données à un tiers constitue un traitement de données distinct du profilage, qui devra être conforme aux principes généraux, voire être justifié par un motif justificatif ; s'alignant sur l'analyse juridique du PFPDT relative aux contrôles de sécurité (*background checks*), l'entreprise qui effectue le profilage dans cette deuxième hypothèse sera qualifiée de « sous-traitant » au sens de l'art. 5 let. k LPD, voir PFPDT, Explications relatives aux contrôles de sécurité (employés du secteur privé), mars 2015.

236 Pour une analyse nuancée du cadre légal qui régit cette hypothèse, voir KASPER/WILDHABER, Big Data am Arbeitsplatz, pp. 195 ss.

données s'appliquera à toutes les candidatures exactement de la même manière. Ainsi, le profilage contribuerait à minimiser les risques de discriminations lorsqu'un employeur choisit un candidat pour un poste donné. Dans ce contexte, on rappellera que les études récentes ont pu montrer que l'entretien d'embauche n'est plus considéré être un moyen efficace afin de recruter les meilleurs collaborateurs, notamment en raison de leur manque d'objectivité[237].

Ensuite, certains auteurs font valoir que le profilage des candidats augmente la satisfaction sur le lieu de travail dans la mesure où les employés déjà embauchés ont la certitude d'avoir été soumis aux mêmes critères d'embauche que les nouveaux-venus[238].

De surcroît, le profilage permettrait d'augmenter l'efficacité du processus de sélection[239], les responsables de ressources humaines n'étant pas amenés à analyser une multitude de dossiers individuels. Il suffirait de s'adresser à un sous-traitant et de lui communiquer les noms des candidats (et parfois de leur transférer les dossiers de candidature) afin de recevoir une évaluation complète des diverses candidatures, y compris une prédiction par rapport aux performances futures. Une telle amélioration de l'efficacité au sein d'une entreprise engendre bien évidemment un avantage concurrentiel.

Enfin, le profilage pourrait contribuer à une augmentation de la sécurité dans le processus de recrutement dans la mesure où les falsifications de documents deviennent de plus en plus simples et qu'environ 25 % des candidatures contiennent des informations erronées[240].

Si le profilage offre certes des avantages, il convient de brièvement résumer les risques engendrés par l'utilisation de ce nouveau traitement de données.

B. Risques

En vertu du Message du Conseil fédéral « on entend par évaluation automatisée toute évaluation fondée sur des techniques d'analyse informatisées. Le recours à des algorithmes est possible mais non constitutif du profilage »[241]. Même s'il

237 À titre d'exemple, on consultera les explications d'IRIS BOHNET, voir ALEXANDER, Harvard-Professorin : « Bewerbungsgespräche sind das schlechteste Instrument, um gute Mitarbeiter*innen zu finden », EDITION F du 5 novembre 2017, <https://editionf.com/interview-iris-bohnet-gleichberechtigung-arbeitswelt/> (dernière consul-tation le 18 janvier 2022).

238 NIKLAS/THURN, p. 1590.

239 KASPER/WILDHABER, Big Data am Arbeitsplatz, pp. 191 s. ; l'augmentation de l'efficacité serait d'ailleurs le but principal de tout traitement de données fondé sur le *Big Data*, voir BERANEK ZANON, p. 87.

240 MORGENROTH, p. 113.

241 FF 2017 6642 ; dans le même sens à propos du profilage en général, c'est-à-dire indépendamment de toute définition légale, voir HILDEBRANDT, p. 17 ; dans le même sens

existe plusieurs définitions possibles du terme « algorithme », il convient, dans le cadre de cette contribution, de s'en tenir à la définition très générale proposée par PODESTA et al. Ainsi, « [traduction] un algorithme est défini par une séquence d'étapes et d'instructions qui peuvent être appliquées à des données »[242]. Sans entrer dans les détails, on rappellera qu'il existe plusieurs sortes d'algorithmes[243]. Dans le contexte du *People Analytics* (et d'autres contextes également) ce sont les algorithmes prédictifs, voire prescriptifs qui suscitent le plus de questions[244]. À ce sujet, l'exemple le plus connu est sans doute celui de la procédure de recrutement automatisée mise en place par l'entreprise américaine *Amazon* en 2014. En effet, le géant du commerce en ligne avait mis au point un logiciel pour procéder à ses recrutements avant de se rendre compte, trois ans plus tard, que celui-ci discriminait les femmes. « Le programme, développé dans le plus grand secret, [...] devait examiner le CV des candidats afin d'automatiser le processus de recrutement en attribuant une note d'une à cinq étoiles selon les profils pour les postes de développeur de logiciel et d'autres postes techniques. [...] En s'appuyant sur l'historique d'*Amazon* qui [a reçu] quasi exclusivement des CV masculins [pendant] dix ans, reflet de la prédominance des hommes dans le secteur des nouvelles technologies, le système en était venu à déduire que les candidats masculins pour ces postes étaient préférables. Cela l'amenait à rejeter les candidatures où figuraient des mots laissant entendre que la candidature était féminine comme la mention 'capitaine de club d'échecs féminin' inscrite dans les loisirs de la candidate [... ou à abaisser] les notes de candidates diplômées d'universités n'accueillant que des femmes »[245]. Ainsi, gardant cet exemple à l'esprit, plusieurs sources d'erreur peuvent être identifiées[246] :

à propos de la définition en droit européen, voir HELFRICH, art. 4 ch. 4 RGPD, N 87 ; pour un avis contraire selon lequel le recours à des algorithmes serait constitutif du profilage en droit européen, voir SPIECKER GENANNT DÖHMANN, p. 350.

242 PODESTA et al., p. 46 ; pour une définition similaire et quelques explications supplémentaires, voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 11.

243 LEICHT-DEOBALD et al. expliquent de manière claire ce qui doit être entendu par « algorithmes descriptifs » (*descriptive algorithms*), « algorithmes prédictifs » (*predictive algorithms*) et « algorithmes prescriptifs » (*prescriptive algorithms*), voir, pour plus de détails et des exemples tirés du monde du travail, LEICHT-DEOBALD et al., pp. 380 s. ; l'ONG *AlgorithmWatch* mentionne quatre sortes d'algorithmes utilisés dans le cadre du *People Analytics* (*diagnostic*, *descriptive*, *predictive* et *prospective analytics*). On notera toutefois que la distinction supplémentaire proposée par les auteurs du rapport n'est sans importance dans le cadre de cette contribution, voir AlgorithmWatch, p. 4.

244 AlgorithmWatch, p. 4.

245 GOLLA, Le logiciel de recrutement d'Amazon n'aimait pas les femmes.

246 Pour plus de précisions quant aux sources d'erreurs et des exemples supplémentaires, voir HEUBERGER, N 29 ss.

D'abord, l'algorithme peut se fonder sur une base de données de mauvaise qualité, c'est-à-dire non représentative (p. ex. si la base de données ne contient que les données des employés ayant participé à une enquête en ligne le risque qu'elle ne contienne avant tout les données de jeunes collaborateurs plus à l'aise avec les questionnaires en ligne ne devrait pas être négligée).

Ensuite, l'algorithme peut évaluer des données erronées (p. ex. si deux personnes portant le même nom et le même prénom figurent dans la base de données[247]).

Après, et comme l'exemple d'*Amazon* a pu le montrer, un algorithme peut également se fonder sur des données stéréotypes ou extraites de leur contexte[248].

Enfin, l'algorithme peut aussi analyser des données historiques et ainsi procéder à une évaluation qui ne correspond plus aux besoins de l'actualité (p. ex. en temps de pandémie, il est facilement concevable que les qualités recherchées pour un poste donné diffèrent de celles qui sont recherchées en « temps normaux ». Ainsi, plus les données collectées sont analysées rapidement, plus la probabilité que l'évaluation obtenue soit correcte est grande[249].

D'un point de vue procédural, il est important de noter que le raisonnement qui sous-tend les algorithmes utilisés afin de déceler des corrélations entre différentes données est de plus en plus complexe et donc de plus en plus difficile à comprendre. Ainsi, dans l'hypothèse où un algorithme se fonderait sur une donnée erronée ou sur une base de données incomplète ou serait programmé de manière, p. ex. discriminatoire, il peut s'avérer très compliqué, voire impossible de comprendre le raisonnement qui sous-tend l'évaluation effectuée de la personnalité du candidat. Engager une procédure contestant l'évaluation proposée par un tel algorithme est alors très difficile. Cet aspect soulève d'importantes questions par rapport au droit fondamental à une procédure équitable, dont le droit de faire l'objet d'une décision compréhensible est partie intégrante[250].

De surcroît, les algorithmes utilisés pour procéder à un profilage sont souvent protégés par diverses dispositions du droit de la propriété intellectuelle[251].

247 À titre d'exemple, MORGENROTH, pp. 31 s. ; en 1988 déjà par rapport à une caisse de recouvrement qui aurait confondu deux personnes portant le même nom et habitant dans la même rue, voir FF 1988 II 457.

248 BÜCHI et al., p. 10.

249 Ce risque est parfois désigné de « Tip Gap Risk », voir BERANEK ZANON, p. 89.

250 Pour un résumé des droits découlant de l'art. 29 al. 2 Cst., qui garantit le droit d'être entendu, voir HÄFELIN/HALLER/KELLER/THURNHERR, N 835 ss.

251 LEICHT-DEOBALD et al., p. 381 ; au niveau européen, le RGPD évoque également cette tension entre le droit d'accès des personnes concernées et le secret d'affaires, voire la propriété intellectuelle, notamment le droit d'auteur protégeant le logiciel, voir RGPD, cons. 63.

Ainsi, même s'il était possible de comprendre le raisonnement qui sous-tend le traitement de données litigieux, p. ex. dans l'hypothèse d'une contestation de l'évaluation effectuée du candidat, il serait très compliqué d'avoir accès à l'architecture de l'algorithme et de la contester le cas échéant[252]. Il découle de ce qui précède que les sources d'erreurs sont multiples lorsque le profilage se fonde sur des algorithmes[253] et que l'opacité du processus d'évaluation peut potentiellement porter atteinte à certaines garanties procédurales.

En fonction des données traitées, voire des corrélations révélées par les algorithmes, le profilage peut par ailleurs porter atteinte à de nombreux intérêts protégés que les droits fondamentaux des candidats ont pourtant vocation à protéger. On pensera au droit au respect de la sphère privée et à l'interdiction de discrimination, mais aussi à de nombreux autres droits fondamentaux, comme p. ex. au droit à une procédure équitable, à la liberté d'expression ou à la liberté de réunion[254]. Le Parlement suisse en était conscient lors de la révision de la LPD dans la mesure où il a défini le « profilage à risque élevé » à l'art. 5 let. g LPD[255].

En raison du flou qui entoure le cadre légal tel que prévu par la LPD, les employeurs qui souhaiteraient recourir au profilage prennent des risques juridiques difficiles à déterminer en amont[256]. En effet, les algorithmes ne jouissant ni de la capacité juridique ni de la capacité civile active, ils ne peuvent être tenus responsables d'une évaluation contraire aux dispositions légales[257]. Ainsi, si un employeur décide d'effectuer un profilage, il sera également responsable d'une évaluation portant atteinte à la personnalité ou aux droits fondamentaux du candidat[258].

Ensuite, le système juridique libéral suisse se fonde, entre autres, sur le concept de la responsabilité individuelle[259]. Ainsi, afin de déterminer si un

---

252 CHRISTL/SPIEKERMANN, pp. 125 s.

253 On rappellera que selon le Message du Conseil fédéral « le recours à des algorithmes est possible mais non constitutif du profilage », voir FF 2017 6642.

254 Voir *supra* Méthodologie.

255 On rappellera que pour des raisons de brièveté, cette contribution analysera uniquement les atteintes potentiellement portées au droit à l'autodétermination en matière informationnelle, qui est une composante du droit au respect de la sphère privée en droit constitutionnel suisse ; pour de plus amples précisions quant à ce choix opéré, voir *supra* Méthodologie.

256 REINSCH/GOLTZ, p. 35.

257 HEUBERGER, N 54.

258 WILDHABER telle que citée dans KAUFMANN/SCHUERCH, Positionspapier, p. 8.

259 MEIER va même plus loin en affirmant que « l'abandon progressif de la causalité au profit de la corrélation, le passage du pourquoi au quoi ou comment, le développement d'un nouveau 'savoir' » remet en cause les « fondements mêmes de notre humanité et

individu est responsable ou non des conséquences d'un acte (ou d'une omission) dans un contexte bien précis, un lien de causalité entre cet acte ou cette omission et sa potentielle conséquence doit pouvoir être établi et l'acte (ou l'omission) doit pouvoir être attribué à l'individu. Ce raisonnement reflète l'approche déductive qui caractérise les sciences juridiques. Ce raisonnement trouve son expression en droit du travail également dans la mesure où il n'est, p. ex., pas permis de licencier, avec effets immédiats, quelqu'un pour des faits qui ne lui sont pas attribuables[260]. En d'autres termes, les art. 336 ss. CO prévoient qu'il est nécessaire d'établir un lien de causalité entre l'acte ou l'omission de l'employé concerné et les conséquences dommageables. On rappellera que la LPD se fonde également sur le principe de causalité et n'a dès lors pas été conçue afin d'encadrer des traitements de données fondés sur des corrélations[261]. Or, l'analyse de données personnelles telle qu'effectuée dans le cadre d'un profilage ne vient pas conforter l'analyse causale que l'employeur aurait pu faire sur la base du dossier de candidature. Un profilage a pour but de rechercher des corrélations entre des données sans s'intéresser au contexte, respectivement au lien de causalité entre deux données personnelles du candidat. Un profilage vise à générer une nouvelle information qui échapperait à une analyse de ces mêmes données effectuée manuellement ou sans l'application d'un algorithme par un employeur. En d'autres termes, le profilage remet en cause le concept de la responsabilité individuelle, qui est au cœur de l'ordre juridique suisse. Cette constatation est d'autant plus vraie que dans une société qui n'accepte de moins en moins les erreurs humaines, l'employeur sera tenté de déléguer une partie, voire toute l'évaluation du candidat à un algorithme et ainsi se décharger – du moins de prime abord – de toute responsabilité dans l'hypothèse où l'embauche s'avérait avoir été une erreur[262].

de notre culture », voir MEIER, Big Data, p. 94 ; dans le même sens, ROUVROY estime que notre responsabilité de rendre compte de nos actions, de nos décisions et de nos intentions en dépit d'éventuelles recommandations ou de profilages effectués sur la base d'algorithmes constitue un « *meta-right* » qu'il convient de protéger dans un État de droit, voir ROUVROY, p. 37 ; pour le Comité des Ministres « cette manière d'attribuer à un individu particulier des données 'à caractère personnel', qui appartiennent en fait à d'autres personnes, crée un phénomène nouveau. En pratique, l'individu est responsable de ses propres actes et se voit imputer de manière sociale ou légale la responsabilité de ceux-ci. Dans le cas du profilage, l'individu se voit attribuer – voire opposer – les données personnelles d'autres individus qu'il ne connaît pas et avec lesquels il ne fait que partager certaines caractéristiques communes », voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 53.

260 À titre d'exemple, voir ATF 131 III 535.

261 HEUBERGER, N 54 ; dans le même sens, MEIER Big Data, p. 91.

262 LEICHT-DEOBALD et al., p. 384.

Dans une veine similaire, on rappellera que les contrats existent afin d'atténuer l'incertitude qui caractérise inévitablement toute transaction. Ainsi, un traitement de données automatisé dont le but consiste à prédire un comportement futur le plus précisément possible vide le contrat envisagé sur la base de cette prédiction de toute son incertitude. Le traitement de données a alors pour conséquence de rendre la nécessité et donc la possibilité de développer un lien de confiance superflues[263]. En d'autres termes, la mise en place d'évaluations automatisées à grande échelle dans le but d'exclure toute incertitude quant au comportement du co-contractant sape le fondement même du droit des contrats.

En outre, le droit au respect de la sphère privée (dont le droit à l'autodétermination en matière informationnelle est une composante[264]) jouit d'un statut particulier dans un État démocratique[265]. Ce droit fondamental est souvent décrit comme un droit fondamental « gate keeper »[266] dans la mesure où la jouissance d'autres droits fondamentaux ne saurait être assurée si la sphère privée des citoyens n'est pas garantie. En d'autres termes, nous ne sommes libres uniquement si nous pouvons contrôler ce que les tiers savent à propos de nous-mêmes[267]. Ainsi, toute personne devrait pouvoir jouir de ses libertés fondamentales sans devoir se demander si l'exercice de ses droits politiques ou de sa liberté de religion impactera ses chances sur le marché du travail, p. ex. en participant à une campagne politique, en se rendant à la mosquée ou en utilisant certaines applications de rencontre qui révéleraient son orientation sexuelle. En d'autres termes, si le profilage est une forme de surveillance mise en place par des particuliers on peut se demander si l'utilisation généralisée du profilage lors du recrutement n'aurait pas, entre autres, pour effet de conduire les personnes à procéder, par principe, à une forme d'autocensure[268] en amont (afin d'augmenter leurs chances sur le marché de l'emploi) et de renoncer ainsi à l'exercice de leurs libertés.

263 ZUBOFF, Big Other, p. 81 ; pour de plus amples développements de cette analyse, voir ZUBOFF, Surveillance Capitalism, pp. 211 ss.

264 Voir *infra* Chapitre 11. Le cadre constitutionnel suisse.

265 MEIER précise que le droit à l'autodétermination en matière informationnelle « constitue également [au-delà de sa portée individuelle] une composante indispensable à l'existence et au développement d'un Etat démocratique », voir MEIER, Protection des données, N 20 avec de nombreuses références supplémentaires.

266 Pour une analyse plus approfondie du statut particulier du droit fondamental à la vie privée, voir GOOLD, pp. 4 ss. ; dans le même sens, voir CUSTERS/URSIC, p. 326.

267 SNYDER, p. 88.

268 Pour une analyse interdisciplinaire des potentiels *chilling effects* du profilage mis en place par des entreprises privées, voir BÜCHI et al., pp. 1 ss.

En sus de ces potentiels *chilling effects* du profilage encore bien trop peu analysés par les chercheurs[269], MEIER s'interroge sur la généralisation du profilage qui pourrait avoir comme conséquence d'exclure, p. ex. du marché du travail, ceux qui souhaiteraient rester hors du système, notamment pour des raisons philosophiques ou politiques (faute de données disponibles à leur égard)[270].

D'un point de vue de la gestion des entreprises, il est fort probable que le profilage sera avant tout utilisé dans les secteurs où les fluctuations du personnel sont fréquentes et dans lesquels les profils des candidats ne se distinguent que peu les uns des autres, comme p. ex. dans le secteur de la gastronomie, des transports ou du commerce de détail[271]. À titre d'exemple, les entreprises comme la *Migros*, les *CFF* ou *Axpo* ont recours aux services de l'entreprise suisse *Livejobs* qui distribue un système de recrutement plus ou moins sophistiqué par vidéo afin de déterminer quels candidats vont être invités à un entretien d'embauche[272]. En d'autres termes, les risques liés à l'utilisation du profilage seront avant tout supportés par les personnes ayant une formation primaire et qui, le plus souvent, doivent vivre avec de bas revenus. Cette tendance est exacerbée en raison de leur standard de vie (en général économiquement défavorisé) qui ne leur permet pas d'être aussi connectées et de générer autant de données que les personnes plus aisées[273]. Ainsi, cette constatation soulève la question plus générale de savoir si l'accès à un entretien d'embauche (et ainsi au marché du travail) avec une personne en chair et en os sera, à l'avenir, un privilège réservé aux classes moyennes, qui évoluent, le plus souvent, dans des secteurs économiques dans lesquels certaines qualités sont requises qui ne sont pas (encore) ou plus difficilement calculables sur la base d'algorithmes[274].

269 BÜCHI et al. déplorent que les quelques publications qui existent à ce sujet portent sur les *chilling effects* des mesures de surveillance mises en place par les pouvoirs publics et non sur le profilage effectué par les acteurs privés, voir BÜCHI et al., p. 13.

270 MEIER, Big Data, p. 93.

271 LEICHT-DEOBALD et al., p. 381 ; dans le même sens, voir CHRISTL/SPIEKERMANN, p. 75 ou GRATWOHL, Bewerbungsgespräche am Laptop : Die Corona-Krise beschleunigt die digitale Rekrutierung, avec une mention particulière de la société d'intérim *Adecco*.

272 On notera que si le programme offert par *Livejobs* offre la possibilité d'effectuer un véritable profilage des candidats (évaluation de certains aspects de la personnalité sur la base de la vidéo enregistrée), reste à savoir si les employeurs cités dans le cadre du reportage de BÜTLER ont activé ou non cette possibilité, voir BÜTLER, Videobewerbung, « Diese Methode ist unmenschlich ».

273 MEIER, Big Data, p. 93.

274 On distinguera cette question de celle de savoir quels emplois risquent d'être les plus touchés par l'IA *pendant* la relation de travail, voir, y compris pour les divergences qui existent quant aux pronostics, OCDE, Social, Employment and Migration Working Papers No. 256, The Impact of Artificial Intelligence on the Labour Market : What Do We Know so Far ?, 25 janvier 2021, pt. 20 ss., et OCDE, Social, Employment and Migration Working Papers No. 265, Artificial Intelligence and Employment : New Cross-Country Evidence, 15 décembre 2021.

Dans le cadre d'un profilage, certains aspects de la personnalité d'un individu sont évalués par une machine. Même si la machine a été programmée par un être humain, l'évaluation automatisée de ces aspects de la personnalité se fera nécessairement de manière schématisée, donc de manière réductrice[275]. On peut se demander s'il n'y a pas, du fait de cette constatation, un risque d'atteinte à la dignité des personnes concernées[276]. Si cette question n'a pas encore reçu de réponse définitive de la part d'une autorité judiciaire[277], elle reste au cœur de l'actualité[278].

Chapitre 6. Conclusion de la première partie

En guise de conclusion de ce chapitre préliminaire, il convient de retenir les six points suivants :

— si la surveillance telle que pratiquée par les *data broker* et exploitée, entre autres, par les employeurs ressemble sur quelques points à celle mise en place par les autorités suisses pendant la Guerre froide (surveillance secrète ; critères d'évaluation inconnus ; conséquences potentiellement néfastes sur les opportunités sur le marché du travail), ces deux formes de surveillance se distinguent sur de nombreux points (but de la surveillance ; catégories et quantité des données traitées ; processus de création de nouvelles connaissances ; nombre de personnes concernées ; sujets de droit concernés ; motifs justificatifs). Dès lors, les nouvelles formes de surveillance mises en place le plus souvent par des particuliers doivent être appréhendées sous un angle différent que les (anciennes) mesures de surveillance utilisées par les pouvoirs publics ;

275 ROSENTHAL, Das neue Datenschutzgesetz, N 26 ; dans le même sens, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 54.

276 BÜCHI et al., p. 16.

277 La Commission européenne a « uniquement » publié un Livre blanc en 2020 dans lequel elle retient que « l'IA peut avoir de nombreux effets positifs, notamment en matière de renforcement de la sécurité des produits et des procédés, mais aussi des effets négatifs. Elle peut être préjudiciable tant sur le plan matériel (en matière de sécurité et de santé des personnes: pertes humaines, dommages aux biens) qu'immatériel (atteinte à la vie privée, restrictions du droit à la liberté d'expression, dignité humaine, discrimination à l'embauche par exemple), et impliquer des risques de types très divers », voir COM(2020) 65 final, p. 12.

278 À juste titre, ROSENTHAL relève que savoir si une évaluation de la personnalité automatisée est, par principe, moins complète que celle effectuée par une personne physique n'est pas une question relevant du droit de la protection des données *stricto sensu*, voir ROSENTHAL, Das neue Datenschutzgesetz, N 107 ; pour un aperçu des développements dans ce domaine qui ont été lancés par l'OCDE, puis repris par le Conseil de l'Europe et, tout récemment par l'UE, voir POULLET, pp. 138 s.

- le profilage est une nouvelle forme de traitement de données qui se déroule en trois étapes techniquement distinctes : après avoir collecté une quantité massive d'observations numérisées de comportements et caractéristiques d'individus (*data warehousing*), ces données sont analysées et soumises à un « forage » (*data mining*) dans le but d'établir des corrélations entre certains comportements ou caractéristiques et d'autres comportements ou caractéristiques. L'étape finale consiste à déduire de nouveaux comportements présents, passés ou futurs ou de nouvelles caractéristiques à partir de certaines variables comportementales ou caractéristiques observables propres à un individu généralement identifié ;
- en droit suisse, le profilage est défini comme toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique. Lorsque le profilage entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de sa personnalité, la nouvelle Loi fédérale sur la protection des données fixe qu'il s'agit d'un « profilage à risque élevé ». On rappellera que le recours à des algorithmes est possible, mais non constitutif du profilage. On rappellera également que les définitions proposées par l'UE et le Conseil de l'Europe peuvent également trouver application en Suisse. Le Législateur helvétique ayant repris la définition européenne du profilage lors de la révision de la LPD, les définitions suisses et européennes sont identiques. La définition prévue dans la Recommandation pertinente du Conseil de l'Europe est désormais alignée sur celles qui sont prévues dans les deux autres dispositifs analysés. Dans le cadre de la révision récente, le Conseil de l'Europe a également introduit une définition de profilage à risque élevé. Cependant, elle diverge fondamentalement de celle prévue en droit suisse ;
- le profilage est un traitement de données qui peut être effectué dans de nombreux contextes. Il peut non seulement être mis en place dans le cadre d'une procédure d'embauche, mais aussi pendant, voire à la fin d'une relation de travail. Ces différentes utilisations du profilage sur le lieu de travail sont souvent désignées sous le nom de *People Analytics*. De plus, le profilage peut être utilisé dans le cadre de nombreuses autres relations juridiques, notamment dans le secteur commercial, bancaire, carcéral ou social, dans le secteur des assurances et de la recherche (médicale), dans la lutte anti-terroriste ou lors de campagnes électorales ;
- lorsqu'un profilage est envisagé au stade de la procédure d'embauche, l'employé type est conçu sur la base d'une analyse automatisée d'une

multitude de données collectées en amont (création du *Perfect Match*). Ensuite, les données relatives au candidat sont comparées au *Perfect Match*. Cette comparaison va permettre d'inférer certaines nouvelles variables comportementales relatives au candidat. Cette évaluation automatisée de certains aspects de sa personnalité est alors vendue à l'employeur intéressé ;

— l'utilisation du profilage dans le cadre d'une procédure d'embauche peut (éventuellement) présenter certains avantages (prises de décision plus objective ; augmentation de l'efficacité ; augmentation de la satisfaction sur le lieu de travail ; prévention de candidatures frauduleuses). Toutefois, certains risques doivent être pris en considération lorsqu'un employeur effectue un profilage dans un tel contexte. Ainsi, si le profilage est effectué sur la base d'algorithmes, plusieurs potentielles sources d'erreurs affectant l'évaluation finale de la personnalité du candidat ont pu être relevées (analyses de données non-représentatives, erronées ou désuètes, voire une conception biaisée de l'algorithme). Au-delà de cette grande variété d'erreurs possibles, on notera qu'il peut s'avérer difficile de déceler ces erreurs, notamment en raison du raisonnement incompréhensible qui sous-tend les calculs de corrélations, du caractère secret de la plupart des profilages et du secret d'affaires qui rend l'accès à l'algorithme (presque) impossible. Ainsi, contester un profilage portant atteinte à la personnalité du candidat est compliqué, voire impossible. Après, l'utilisation du profilage remet en cause certains concepts fondamentaux de notre ordre juridique, notamment la responsabilité civile qui veut que l'individu est responsable de ses propres actes et se voit imputer de manière sociale ou légale la responsabilité de ceux-ci. En revanche, dans le cadre du profilage, l'individu se voit attribuer (voire opposer) les données personnelles d'autres individus qu'il ne connaît pas et avec lesquels il ne fait que partager certaines caractéristiques communes. De surcroît, un profilage effectué entre privés peut potentiellement porter atteinte à divers intérêts protégés par les droits fondamentaux de la personne concernée ce qui soulève de nombreuses questions épineuses quant à la portée des droits fondamentaux entre privés. Dans ce contexte, on rappellera que le profilage constitue une forme de surveillance. Une généralisation du profilage pourrait alors conduire à une forme d'autocensure des individus inquiets de perdre une opportunité sur le marché du travail s'ils font trop généreusement usage de leurs droits et libertés. En d'autres termes, la mise en place de plus en plus de mesures de surveillance, notamment par des particuliers, pourrait restreindre l'exercice de nos droits et libertés de manière plus généralisée. Dans une veine similaire, se pose également

la question (à ce jour restée sans réponse définitive) si le fait qu'un candidat soit soumis à une évaluation schématisée, donc incomplète de sa personnalité, constitue une atteinte à sa dignité. Enfin, il est fort probable que le profilage soit avant tout utilisé dans les secteurs économiques où les fluctuations du personnel sont fréquentes et dans lesquels les profils des candidats ne se distinguent que peu les uns des autres. Ainsi, se pose la question plus générale de savoir si l'accès à l'évaluation de la personnalité d'un candidat par une personne physique sera réservé, dans le futur, aux candidats de la classe moyenne, voir supérieure évoluant souvent à des postes pour lesquels une évaluation automatisée, donc forcément schématisée et réductrice de la candidature, est insuffisante.

Après avoir défini la notion principale utilisée dans le cadre de cette contribution et présenté les avantages et les risques liés à l'utilisation du profilage, il convient de se pencher sur le cadre légal du profilage dans le cadre d'une procédure d'embauche et de vérifier si ce cadre légal permet de contrer les risques auxquels les personnes concernées font face.

Partie 2. L'encadrement lacunaire du profilage par les lois fédérales

Un employeur, qui souhaite effectuer le profilage d'un candidat se voit dans l'obligation de respecter plusieurs lois fédérales.

D'abord, l'employeur doit veiller au respect du cadre légal fixé, de manière très générale, par les dispositions du Code des obligations[279] (ci-après « CO ») régissant le contrat de travail (chapitre 7). Les dispositions pertinentes en matière de traitements de données personnelles renvoient, pour les détails, à la Loi sur la protection des données[280] (ci-après « LPD »). Dans un deuxième temps, il conviendra dès lors de se pencher sur les dispositions de la LPD applicables en la matière (chapitre 8). Ensuite, les dispositions pertinentes de la Loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (ci-après « LHand »)[281] ainsi que celles de la Loi fédérale sur l'égalité entre femmes et hommes[282] (ci-après « LEg ») doivent être respectées dans le cadre de nombreuses procédures d'embauche. Enfin, il convient de noter que la Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce[283] (ci-après « LTr »), l'Ordonnance 3 relative à la loi sur le travail (Protection de la santé)[284] (ci-après « OLT 3 ») et le Code pénal[285] (ci-après « CP ») contiennent potentiellement quelques dispositions qui doivent être respectées lorsqu'un employeur procède à un traitement de données personnelles dans le cadre d'une procédure d'embauche (chapitre 9).

279 Loi fédérale complétant le Code civil suisse (Livre cinquième : Droit des obligations) (CO) du 30 mars 1911, RS 220.

280 Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, RS 235.1.

281 Loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (LHand) du 13 décembre 2002, RS 151.3.

282 Loi fédérale sur l'égalité entre femmes et hommes (LEg) du 24 mars 1995, RS 151.1.

283 Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce (LTr) du 13 mars 1964, RS 822.11.

284 Ordonnance 3 relative à la loi sur le travail (Protection de la santé) (OLT 3) du 18 août 1993, RS 822.113.

285 Code pénal suisse (CP) du 21 décembre 1937, RS 311.0.

Dès lors, il convient de préciser le cadre légal fixé par ces diverses dispositions fédérales. Dans une veine plus concrète, cette deuxième partie a pour but de rechercher si un employeur établi en Suisse peut effectuer un profilage d’un candidat et si tel est le cas, quelles limites légales doivent être respectées.

Chapitre 7.
Le Code des obligations

Contrairement à d'autres ordres juridiques européens[286], la Suisse ne dispose pas d'un Code du travail qui vient encadrer les relations (individuelles et collectives) entre les employeurs privés et leurs employés. Ainsi, les art. 319 CO à 330a CO régissent le contrat de travail en tant que sous-espèce du contrat, au même titre, p. ex., que la donation ou le prêt. Ainsi, il va sans dire que le contrat de travail suisse – du moins en comparaison avec les régimes légaux de certains pays voisins – n'est pas soumis à une multitude de règles précises. En d'autres termes, les dispositions du CO pertinentes en matière de profilage ne sont que peu nombreuses et formulées de manière très vague. D'une part, l'art. 328 CO fixe qu'il incombe à l'employeur de veiller au respect de la personnalité du travailleur (A). D'autre part, l'art. 328b CO encadre les traitements de données personnelles licites (B).

A. La protection de la personnalité du travailleur (art. 328 CO)

L'art. 328 al. 1er CO fixe que « l'employeur protège et respecte [...] la personnalité du travailleur ; il manifeste les égards voulus pour sa santé et veille au maintien de la moralité ». Le deuxième alinéa nuance ce principe en prévoyant qu'« il [l'employeur] prend, pour protéger la vie, la santé et l'intégrité personnelle du travailleur, les mesures commandées par l'expérience, applicables en l'état de la technique, et adaptées aux conditions de l'exploitation ou du ménage, dans la mesure où les rapports de travail et la nature du travail permettent équitablement de l'exiger de lui ».

Cette disposition à laquelle il ne peut être dérogé au détriment de l'employé[287] vient préciser la portée de la protection de la personnalité telle que consacrée aux art. 27 et 28 Code civil[288] (ci-après « CC ») dans le cadre des relations de travail[289]. L'obligation de l'employeur de protéger la personnalité de

286 À titre d'exemple, on pensera aux Codes du travail français et luxembourgeois.

287 Art. 362 CO.

288 Code civil suisse (CC) du 10 décembre 1907, RS 210.

289 PELLASCIO, art. 328 CO, N 8 ; HUGENTOBLER, art. 328 CO, N 3 ; à juste titre, TRUTMANN explique que l'art. 328 CO vient préciser la portée de la protection garantie par les art. 27 et 28 CC dans les relations de travail et non étendre ladite protection, voir TRUTMANN, p. 467.

l'employé doit être comprise comme un des divers aspects de son devoir d'assistance, au même titre, p. ex. que son obligation de protéger les données personnelles de l'employé (art. 328b CO) ou celle de garantir l'égalité entre femmes et hommes (art. 3 LEg)[290].

L'art. 328 CO vient protéger divers biens juridiques dont les contours sont sujets à de constants changements en raison de l'évolution de l'opinion dominante[291] et des développements scientifiques et technologiques[292]. Aujourd'hui, il est admis que cette disposition vient protéger l'honneur professionnelle et privée, la réputation professionnelle, l'intégrité physique et psychique, les sphères privée et intime, la liberté d'expression et la liberté syndicale[293]. Dans ce contexte, il convient de noter que les mesures de surveillance *permanentes*, comme p. ex. un profilage ininterrompu *pendant* une relation de travail, sont considérées porter atteinte à l'intégrité psychique des personnes concernées et sont dès lors interdites[294].

Deux obligations incombant à l'employeur découlent de cette disposition : une obligation positive de prendre toute mesure apte à protéger la personnalité de l'employé (p. ex. mise en œuvre de mesures contre le mobbing au sein de l'entreprise[295]) et une obligation négative de porter le moins possible atteinte à cette personnalité[296] (p. ex. en ne traitant aucune donnée de santé relative à l'employé[297]). Le respect de ces obligations s'apprécie toujours au cas par cas à la lumière du principe de la bonne foi[298]. De plus, il convient de ne pas oublier que les droits fondamentaux déploient un éventuel effet horizontal à travers l'art. 328 CO. En d'autres termes, les contours des diverses obligations de l'em-

290 EMMEL, art. 328 CO, N 1 ; HUGENTOBLER, art. 328 CO, N 1.

291 PELLASCIO, art. 328 CO, N 10.

292 TRUTMANN, p. 466.

293 HUGENTOBLER, art. 328 CO, N 3 ; EMMEL, art. 328 CO, N 2 ; DUNAND, art. 328 CO, N 13 ss.

294 HUGENTOBLER renvoie, à juste titre, à l'interdiction de principe fixée à l'art. 26 al. 1er OLT 3 sans pour autant oublier que cette interdiction supporte quelques exceptions délimitées à l'al. 2, voir HUGENTOBLER, art. 328 CO, N 11.

295 D'un autre avis, avant tout quant aux mesures qui devraient être mises en place pour « humaniser » le lieu de travail, voir TRUTMANN, pp. 467 s. ; pour une analyse de la jurisprudence du Tribunal fédéral relative au mobbing sur le lieu de travail, voir ABEGG, art. 328 CO, N 9 et EMMEL, art. 328 CO, N 5.

296 PELLASCIO précise, à juste titre, que les obligations positives doivent être admises avec plus de retenue que les obligations négatives, voir PELLASCIO, art. 328 CO, N 4 ; dans le même sens, voir FAVRE/MUNOZ/TOBLER, art. 328 CO, N 1.1.

297 HUGENTOBLER, art. 328 CO, N 8. Au vu des enjeux liés à la pandémie du Covid-19, il semble que cette position mérite d'être nuancée.

298 PELLASCIO, art. 328 CO, N 3 ; HUGENTOBLER, art. 328 CO, N 1.

ployeur se détermineront non seulement à la lumière du principe de la bonne foi, mais aussi à la lumière de la jurisprudence constitutionnelle pertinente[299].

Le profilage (même ponctuel) constitue une forme de surveillance[300] et peut ainsi porter atteinte à la personnalité du candidat. À première lecture, cette disposition semble donc encadrer cette forme de traitement de données personnelles. Toutefois, fait encore débat de savoir si cette disposition est applicable dans le cadre d'une procédure d'embauche. En effet, STAEHELIN fait valoir que cette disposition ne s'applique qu'une fois la relation de travail entamée, voire éventuellement à partir du moment où le contrat de travail est signé. Dès lors, les potentielles atteintes à la personnalité du candidat seraient soumises au régime de la *culpa in contrahendo*[301]. Dans une veine similaire, mais moins explicite, ABEGG précise que cette disposition, dans son volet temporel, s'applique du début à la fin de la relation de travail. Ainsi, une telle position semble laisser entendre que la disposition ne devrait pas trouver application avant le début (formel) de la relation de travail[302]. Cette approche semble d'ailleurs découler du texte lui-même qui prévoit qu'il incombe à l'employeur de veiller au respect de la personnalité de l'employé « *dans* les rapports de travail ».

Au contraire, TRUTMANN est d'avis que déjà lors des entretiens en vue de la conclusion d'un contrat de travail, le respect de la personnalité du travailleur prescrit par l'art. 328 al. 1er CO s'impose, notamment parce qu'il est également exigé par les art. 27 et 28 CC et que la relation de confiance particulière généralement reconnue pour la négociation d'un contrat se caractérise par les mêmes obligations que celles propres au contrat à conclure[303]. PELLASCIO partage la

299 PELLASCIO, art. 328 CO, N 8 ; pour des précisions sur comment articuler l'application de deux droits fondamentaux contradictoires par le biais d'une telle disposition de droit privé « perméable » à diverses libertés, voir MARTENET, La protection, p. 427.

300 WALTER, Le profilage, p. 94.

301 STAEHELIN, art. 328 CO, N 12 ; dans le même sens par rapport à l'arrêt du Tribunal des prud'hommes de Lausanne du 1er juin 2005 qui portait sur un refus d'embauche en raison de la couleur de peau de la candidate et qui se fondait, à tort selon les auteurs, sur l'art. 328 CO, voir WYLER/HEINZER, pp. 83 s. ; MARTENET quant à lui précise à propos de cette même affaire que « les parties n'étaient liées par aucun rapport de travail et [que] la société défenderesse n'avait posé aucune question portant atteinte à la personnalité de la candidate. De plus, la société avait rapidement fait part de sa détermination, ce qui permet difficilement de lui reprocher une *culpa in contrahendo*. [Selon cet auteur], cette cause aurait pu permettre au Tribunal saisi […] de poser une règle prétorienne », voir MARTENET, La protection, p. 428.

302 ABEGG précise que « [traduction] l'obligation de mettre en place des mesures de protection s'applique en principe du début à la fin de la relation de travail », voir ABEGG, art. 328 CO, N 6.

303 TRUTMANN, p. 472.

conclusion de TRUTMANN sans pour autant préciser quelles réflexions l’ont poussé à aboutir à cette conclusion[304]. S’il est vrai qu’une telle lecture de cette disposition semble être moins fidèle à la lettre du texte que celle proposée par STAEHELIN et ABEGG, elle semble pourtant mieux refléter la dynamique qui caractérise la majorité des procédures d’embauche en pratique. En effet, la procédure d’embauche est souvent ressentie comme une première phase de la relation de subordination caractéristique de la relation de travail, le candidat souhaitant satisfaire les attentes de l’employeur non seulement pendant la relation de travail, mais aussi (et surtout) pendant la procédure de recrutement[305].

Sur la base de la littérature consultée, il semble que le Tribunal fédéral n’a pas (encore) rendu de décision à ce sujet[306]. Au vu des risques tant pour la personnalité que pour certains droits fondamentaux des candidats, il est à espérer qu’une autorité judiciaire étende le champ d’application *ratione temporis*, voire se fonde sur cette disposition afin de reconnaître certains effets horizontaux aux droits fondamentaux invoqués par les personnes concernées[307]. En effet, l’art. 328 CO garantit que certains droits fondamentaux puissent déployer des effets dans les relations de travail entre privés[308]. Ainsi, c’est dans une affaire établissant le droit du travailleur de consulter son dossier personnel, que le Tribunal fédéral a introduit la notion d’ « autodétermination informationnelle » et qu’il a précisé qu’un tel droit d’accès faisait partie de ce droit[309].

304 PELLASCIO écrit que « [traduction] la personnalité du travailler doit également être protégée dans le temps : lors de la procédure d’embauche et après la fin de la relation contractuelle », voir PELLASCIO, art. 328 CO, N 8.

305 TRUTMANN, p. 472.

306 Pour les diverses raisons pour lesquelles la jurisprudence à propos de cette question est inexistante, voir TRUTMANN, pp. 468 et 475 ; Le Tribunal fédéral et la Cour EDH se sont toutefois penchés plusieurs fois sur la portée de cette disposition *après* la fin de la relation de travail, voir, à titre d’exemple, ATF 4A_117/2013, cons. 2.2 ; ATF 135 III 405, cons. 3.2 ; ATF 130 III 699, cons. 5.1 et, pour une brève analyse de la jurisprudence de la Cour EDH et de son (potentiel) impact sur la fin des relations de travail en Suisse, voir BERSET BIRCHER/MEIER, pp. 612 ss.

307 Faisant référence à l’interdiction constitutionnelle de discrimination, MARTENET précise qu’« il convient évidemment de saluer les efforts récents consistant à développer une jurisprudence novatrice en la matière. Ils ne sauraient toutefois masquer le fait que l’ordre juridique suisse demeure lacunaire », voir MARTENET, La protection, p. 427. Ce constat n’est pas seulement pertinent quant à la protection des discriminations entre particuliers, mais également quant à la protection de l’autodétermination en matière informationnelle entre particuliers, voir FLÜCKIGER, p. 862.

308 À propos de la portée de l’interdiction constitutionnelle de discrimination sur le lieu de travail, voir MARTENET, La protection, pp. 419 ss., avant tout pp. 426 ss. avec de multiples références supplémentaires.

309 MÉTILLE, Le droit au respect de la vie privée, p. 31 ; ATF 120 II 118.

Mis à part l'art. 328 CO, il ne reste qu'une disposition dans le CO qui pourrait encadrer le profilage dans le cadre d'une procédure d'embauche : l'art. 328b CO.

B. Le traitement de données personnelles (art. 328b CO)

L'art. 328b CO, introduit dans le CO lors de l'adoption de l'aLPD en 1992, se lit comme suit : « L'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables ».

Reprenant les mots de MATHIS-ZWYGART, « l'introduction de l'art. 328b CO avait pour but de protéger la personnalité du travailleur au moyen d'une disposition de protection des données spécifique. Il a également été jugé nécessaire d'étendre la portée de l'art. 362 CO en complétant la liste des dispositions du code [des obligations] auxquelles il ne peut être dérogé au détriment du travailleur. Ces compléments apportés à la législation sur le contrat de travail ont été qualifiés d'indispensables car le rapport de travail, plus que n'importe quel autre rapport juridique, donne lieu à la collecte et au traitement de données personnelles de toute nature et pendant une longue durée. Il se justifiait en conséquence d'accorder une protection particulière au travailleur, d'autant plus que celui-ci dépend en fait et en droit de son employeur »[310].

Ainsi, en 1988 déjà, le Législateur souhaitait éviter que les nouvelles formes de traitements de données personnelles rendent les employés « transparents »[311]. Ce but de nature abstraite devait être atteint grâce à l'introduction d'une définition plus restrictive du principe de proportionnalité dans les relations de travail[312]. Ainsi, l'art. 328b CO devient *lex specialis* par rapport à l'art. 4 al. 2 aLPD[313].

Dès lors, l'employeur ne peut qu'effectuer des traitements de données en lien direct avec la procédure de recrutement. Tout traitement de données dépourvu de ce lien constitue alors une atteinte à la personnalité. Il découle de

310 MATHIS-ZWYGART, p. 310 ; dans le même sens, en 1983 déjà, voir TRUTMANN, p. 470.

311 STAEHELIN précise que cet « [traduction] article (...) concrétise le principe de proportionnalité (...) dans le but d'empêcher que le travailleur devienne complètement 'transparent' » (*vollständige Durchleuchtung*), voir STAEHELIN, art. 328b CO, N 1.

312 PELLASCIO, art. 328b CO, N 2.

313 STAEHELIN, art. 328b CO, N 1. Aujourd'hui, le principe de proportionnalité est consacré à l'art. 6 al. 2 LPD.

cette constatation qu'un traitement de données en principe licite en vertu du principe de proportionnalité « général » consacré dans la LPD peut être disproportionné dans le cadre d'une procédure d'embauche[314]. En raison de la nature contraignante de l'art. 328b CO, même le consentement du candidat concerné ne saurait alors justifier un traitement de données allant au-delà du cadre fixé par cette disposition[315]. En d'autres termes, l'art. 328b CO vient inverser la logique générale applicable en droit de la protection des données suisse (principe du *opt-out*) : en principe, un traitement de données personnelles dans le cadre d'une procédure d'embauche est interdit. Un tel traitement peut exceptionnellement être effectué s'il est nécessaire à la conclusion du contrat[316].

Dans un deuxième temps on peut se demander ce qui doit être entendu par « traitement nécessaire » au sens de l'art. 328b CO. La nécessité d'un traitement envisagé s'appréciera toujours sur la base d'une analyse objective du cas d'espèce[317]. L'appréciation subjective du critère de nécessité proposée par certains auteurs[318] ne saurait convaincre dans la mesure où la tentation de l'employeur d'en savoir (toujours) davantage sur le candidat est grande. En d'autres termes, une appréciation subjective ne semble pas être apte à limiter les traitements de données dans le cadre de procédures d'embauche à ce qui est strictement nécessaire.

Une exception à cette limitation semble toutefois être justifiée pour les traitements de données de candidats à des postes au sein d'entreprises de tendance ou à haute responsabilité[319]. Une évaluation (automatisée ou pas) extensive de la personnalité de ces candidats pourrait, si toutes les autres conditions

314 STAEHELIN, art. 328b CO, N 1 avec des références supplémentaires allant dans le même sens.

315 REHBINDER/STÖCKLI, art. 328b CO, N 12.

316 On notera que cette analyse reflète l'approche qui semble dominer en doctrine. Une minorité défend une approche plus libérale et considère que l'art. 328b CO ne consacre pas une interdiction de principe, mais plutôt un principe général supplémentaire qui serait applicable en droit du travail et dont la violation pourrait, par conséquent, être justifiée par un des quatre motifs justificatifs consacrés dans la LPD, voir pour un résumé de ces deux approches et de multiples références supplémentaires, KASPER/WILDHABER, pp. 196 ss. ; pour une analyse critique de cette interprétation jurisprudentielle consacrée par le Tribunal des prud'hommes zurichois le 22 janvier 2016, voir VASELLA, qui défend, à titre d'exemple, l'approche plus libérale, voir VASELLA, OR 328b als eigenständige Verbotsnorm ohne Rechtfertigungsmöglichkeit.

317 PÄRLI, art. 328b CO, N 21 ; PELLASCIO, art. 328b CO, N 7 ; STAEHELIN, art. 328b CO, N 5 ; EMMEL, art. 328b CO, N 4.

318 BRÜHWILER, p. 243.

319 REHBINDER/STÖCKLI, art. 328b CO, N 5 ; STAEHELIN, art. 328b CO, N 5.

sont remplies, se justifier au regard de la nature des tâches envisagées. Or, comme nous l'avons vu plus haut déjà, le profilage est actuellement avant tout effectué pour recruter des candidats avec une formation primaire. Ces candidats ne disposant pas de la formation nécessaire afin d'assumer un poste à haute responsabilité, il ne semble pas être nécessaire de rendre cette catégorie de candidats « transparents »[320]. Dès lors, le profilage effectué dans le cadre d'une procédure d'embauche ne semble pas être conforme aux exigences de l'art. 328b CO[321]. De plus, on rappellera que le régime mis en place reste peu efficace, notamment en raison des difficultés liées à la preuve de l'atteinte[322].

Pour toutes les autres questions liées au traitement de données dans le cadre d'une procédure d'embauche, l'art. 328b CO renvoie à la LPD. DAEDELOW déplore cette « double admissibilité » (*Doppelzulässigkeit*) en droit du travail qui implique que les traitements de données effectués par l'employeur doivent non seulement être conformes à l'art. 328b CO, mais aussi à la LPD. Elle regrette, à juste titre, que les travaux de révision n'aient pas considéré la consécration d'une disposition similaire à l'art. 88 RGPD, qui permet au Législateur national d'adopter, en droit national, une disposition qui encadre les traitements de données sur le lieu de travail d'un point de vue de la protection des données (LPD) *et* de la protection de la santé psychique (OLT 3) simultanément[323]. Cela étant, à défaut d'une telle disposition en droit suisse, les principes généraux ainsi que les sanctions pénales prévus par la LPD sont donc également applicables dans le cadre de procédures de recrutement. Dès lors, il convient de se pencher sur le régime général prévu par la LPD.

320 Dans ce contexte, on rappellera que « le [TAF] a admis une mesure de requête de mesures provisionnelles du [PFPDT] tendant à ce qu'une société renonce à fournir aux entreprises des renseignements sur les candidats à l'embauche. Les données communiquées aux futurs employeurs comportaient des profils de personnalité [au sens de l'aLPD] et portaient notamment sur la situation financière, la vie privée, les poursuites ou encore l'âge et le sexe de la personne avec qui le candidat faisait ménage commun », voir DUNAND, art. 328b CO, N 58 et TAF A-8028/2008 du 14 janvier 2009, *Mitarbeiter-Check* respectivement.

321 Pour une analyse extensive du respect du principe de proportionnalité d'un profilage effectué dans le cadre d'une procédure d'embauche, voir *infra* Chapitre 8. La Loi sur la protection des données.

322 Cette constatation à propos de la LPD et de la LEg est reprise de LEMPEN, mais vaut, à mon sens, *mutatis mutandis* également pour l'art. 328b CO, voir LEMPEN, p. 278.

323 DAEDELOW rappelle de surcroît que cette double admissibilité est également consacrée à l'art. 26 OLT 3 qui fixe le cadre des mesures de surveillance licites sur le lieu de travail, voir DAEDELOW, p. 37.

Chapitre 8.
La Loi sur la protection des données

Comme nous allons le voir par la suite, on peut se demander s'il était nécessaire de définir le nouveau traitement de données connu sous le nom de profilage dans la nouvelle LPD et si oui, comment il convenait de procéder, a fait couler beaucoup d'encre et a suscité de vifs débats au Parlement[324]. Ainsi, afin de mieux comprendre le nouveau régime encadrant le profilage, il convient de se pencher, de manière critique, sur la genèse de cette nouvelle définition qui vient remplacer celle de « profil de la personnalité », notion qui était consacrée à l'art. 3 let. d de l'ancienne Loi sur la protection des données[325] (ci-après « aLPD ») et qui, hormis son nom, n'a que peu en commun avec le profilage (A). Étant donné que tout employeur qui souhaite recourir au profilage ne devra, bien évidemment, non seulement tenir compte de la définition légale du profilage, mais aussi des diverses autres dispositions de la LPD, il n'est pas suffisant d'analyser la nouvelle définition du profilage (B). En effet, les limites imposées au profilage par les principes généraux (C) et les éventuels motifs justifiant un profilage qui serait jugé contraire à l'un des principes généraux (D) devront dès lors également être abordés. Enfin, et faisant référence à ce qui a pu être décrit au chapitre 2, le Législateur suisse s'est inspiré de la définition du profilage consacrée en droit européen. Ainsi, après un bref résumé du régime juridique suisse actuellement en vigueur (E), il convient de terminer ce chapitre avec une analyse de ce qui a pu être décidé au niveau européen (F) afin de s'en inspirer lors de la mise en œuvre de la LPD.

A. Quelques remarques préliminaires

Ni l'aLPD ni une quelconque loi cantonale sur la protection des données[326] ne prévoyait une définition du profilage. Toutefois, l'art. 3 let. e aLPD venait encadrer « toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, […] l'exploitation, la

324 STENGEL/STÄUBLE, N 7 ss. ; ROSENTHAL, Das neue Datenschutzgesetz, N 3 ; MÉTILLE, La (nouvelle) loi fédérale, p. 26 ; POWELL, N 12.

325 Loi fédérale sur la protection des données du 19 juin 1992, RS 235.1, abrogée le 31 août 2023.

326 La Constitution suisse ne consacre pas une compétence exclusive à la Confédération en matière de protection des données. Les cantons restent donc compétents pour la protection des données lorsqu'ils traitent des données personnelles dans un de leurs domaines de compétence. Ainsi, à titre d'exemple, le traitement de données personnelles par les hôpitaux ou les écoles publics est soumis au contrôle des préposés cantonaux, voir BELSER, § 5, N 42 ss. Au regard des développements au niveau tant fédéral qu'euro-

modification [...] de données ». Ainsi, malgré une jurisprudence inexistante[327] et un Message du Conseil fédéral de 1988 (évidemment) muet à ce sujet, l'aLPD semblait englober le profilage. Toutefois, à y regarder de plus près, le profilage échappait aux dispositions de l'aLPD dans la mesure où le droit d'accès (art. 8 aLPD) et le devoir d'information (art. 14 aLPD) impliquaient l'existence d'un fichier (physique). Or, les nouvelles technologies permettent d'exploiter des données comme un fichier, alors même qu'elles sont disséminées dans plusieurs bases de données[328].

En décembre 2011, le Conseil fédéral a approuvé un premier rapport sur l'évaluation de l'aLPD[329] et a chargé le Département fédéral de justice et police (ci-après « DFJP ») d'examiner l'opportunité de renforcer la législation en matière de protection des données. Le DFJP a été chargé de tenir compte, dans ses travaux, des résultats de l'évaluation et des développements en cours au sein de l'UE et du Conseil de l'Europe et de faire des propositions concernant la marche

péen, certains cantons ont modifié leur loi cantonale, d'autres ont lancé la procédure de révision, notamment afin de contribuer à ce que l'UE puisse rendre sa décision d'adéquation. Fin mai 2021, un tiers des cantons suisses environ avaient terminé la révision de leur loi cantonale. Tous les cantons ont inclus, dans la version révisée de leur loi cantonale, une définition du profilage. Étant donné que le profilage à risque élevé n'a qu'une portée dans les relations entre particuliers (exclusivement régies par le droit fédéral), les cantons ont, à juste titre, renoncé à introduire la définition de profilage à risque élevé dans leur loi cantonale. Les développements législatifs dans les cantons de Glaris et Appenzell Rhodes-Intérieures méritent d'être mentionnés : les lois cantonales respectives ne se contentent pas de définir le profilage, mais prévoient que le résultat du profilage, c'est-à-dire le résultat de l'évaluation automatisée, doit être soumis au même régime légal que le traitement de données sensibles, voir POWELL, N 7, 14 s. Tel n'est pas le cas au niveau fédéral. En effet, les restrictions imposées aux traitements de données sensibles ne s'appliquent pas aux évaluations automatisées de certains aspects personnels relatifs à une personne physique, voir, sans prétendre à l'exhaustivité, les art. 30 al. 2 let. c et 31 al. 2 let. c LPD. Toutefois, dès qu'un profilage conduit à l'obtention de données personnelles sensibles, le régime fédéral renforcé s'applique, voir FF 2017 6642. En d'autres termes, les deux régimes cantonaux susmentionnés n'englobent pas une multitude de constellations supplémentaires ; dans le même sens déjà avant l'entrée en vigueur de la nLPD, voir MEIER, Big Data, p. 59.

327 MÉTILLE fait notamment valoir que « le faible nombre de cas portés devant les tribunaux ne tient pas à une situation idéale mais aux embûches, notamment financières, pour faire valoir les droits garantis par la LPD », voir MÉTILLE, Jurisprudence actuelle, p. 114 ; dans le même sens, voir MEIER, Protection des données, N 1718 et FÜZESSÉRY/SCHNEIDER, p. 156 ; pour la même constatation quant à la situation en Suisse *et* au sein de l'UE (sous le régime de la DPD désormais abrogée et remplacée par le RGPD), voir CELLINA, L'influence des réformes européennes, p. 223 ; LEMPEN quant à elle explique ce faible nombre de cas par « le fait que ces lois [la LPD et la LEg] traitent d'un même problème 'parallèlement' en droit public et en droit privé [rendant] leur maîtrise difficile – eu égard aux spécificités propres à chaque régime – et ne favorise probablement pas le recours à ces instruments juridiques en justice », voir LEMPEN, p. 278.

328 Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données, pt. 8.1.1.3 ; FF 2017 6643 s. ; dans le même sens, voir HEUBERGER, N 48 ss. avec de plus amples explications.

329 FF 2012 255.

à suivre avant la fin 2014. Afin de mieux cerner les nouveaux défis et de mieux répondre aux intérêts des différents groupes de personnes concernées, un groupe d'accompagnement a été mis en place, qui a publié ses conclusions dans un rapport fin 2014[330]. En août 2016, un avant-projet de loi[331] accompagné d'un rapport explicatif[332] a été soumis au Conseil fédéral. Cet avant-projet se fondait et sur le premier rapport sur l'évaluation de l'aLPD du Conseil fédéral et sur le rapport du groupe d'accompagnement mis en place par l'OFJP. Après la consultation relative à l'avant-projet[333], le Conseil fédéral a adopté le Message relatif à la révision totale de l'aLPD le 15 septembre 2017[334].

Il convient de noter que savoir s'il fallait légiférer en matière de profilage et si oui, sous quelle forme, n'a pas été abordé dans le premier rapport publié en 2011. Ainsi, dans le rapport du Conseil fédéral du 9 décembre 2011 la notion de « profilage » n'est jamais employée, la notion de « décision automatisée » n'apparaît uniquement dans le cadre des résumés des travaux du Conseil de l'Europe et de leur impact sur le droit suisse. Cela étant, le Conseil fédéral a néanmoins reconnu il y a plus de dix ans déjà, qu'il convenait, d'« assurer la protection des données (…) dès la conception de nouvelles technologies (…) et d'améliorer le contrôle et la maîtrise des données »[335].

Quelques années ont pourtant suffi à ce qu'en 2014, le groupe d'accompagnement Révision LPD consacre une partie de ses réflexions à une définition possible du profilage. Dans son rapport publié en octobre 2014, il écrit que « de plus en plus souvent, des décisions produisant des effets juridiques pour les personnes concernées ou pouvant les affecter de manière significative sont

330 Office fédéral de la justice (OFJ), Domaine de direction Droit public, Unité Projets et méthode législatifs, Esquisse d'acte normatif relative à la révision de la loi sur la protection des données, Rapport du groupe d'accompagnement Révision LPD du 29 octobre 2014 ; le groupe d'accompagnement comprenait des représentants de l'administration fédérale, des cantons, des milieux scientifiques ainsi que des organisations de l'économie et des consommateurs, pour une liste exacte des membres du groupe d'experts, voir n 2, pp. 3 s. dudit rapport.

331 Office fédéral de la justice (OFJ), Projets législatifs en cours, Renforcement de la protection des données.

332 Office fédéral de la justice (OFJ), Domaine de direction Droit public, Unité Projets et méthode législatifs, Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016.

333 Une synthèse des résultats de la procédure de consultation a été publiée par l'OFJ le 10 août 2017, voir Office fédéral de la justice (OFJ), Synthèse des résultats de la procédure de consultation.

334 FF 2017 6565.

335 FF 2012 268.

prises dans le cadre de procédures automatisées, voire sur la base de profils reposant sur des données statistiques et des calculs (profilage). Une majorité du groupe d'accompagnement estime qu'il y a un besoin accru de protection en particulier lorsque de telles procédures de décision portent sur les caractéristiques d'une personne, par exemple sa solvabilité, sa fiabilité, son comportement ou des risques spécifiques »[336]. Le groupe d'accompagnement semble aborder les problématiques liées aux nouveaux traitements de données en partant de la notion de « décision individuelle automatisée ». Ainsi, il poursuit en écrivant qu'« il faut encore examiner [lors de la révision de l'aLPD] plus précisément quelles procédures doivent être qualifiées de décisions automatisées au sens décrit »[337]. Une minorité du groupe aurait pourtant préféré adopter une approche aux nouvelles problématiques axée sur les droits à accorder aux personnes concernées. En effet, il est précisé dans le rapport qu'« une minorité du groupe d'accompagnement souhaite que [la LPD révisée] doit être complétée par un droit de s'opposer au profilage prédictif automatisé » étant donné que les « profils qui en résultent peuvent en effet entraîner des erreurs d'appréciation ou des discriminations »[338]. Il ne ressort pas du rapport quels arguments ont poussé les différents membres du groupe à s'aligner sur la position de la majorité, respectivement sur celle de la minorité.

Deux ans plus tard, le rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données mentionne, parmi les grandes lignes de la révision, la nécessité de remplacer la notion de « profil de la personnalité » par celle de « profilage »[339], propose une définition du profilage qui ressemble à celle qui a été prévue en droit européen et soulève, à juste titre, plusieurs limites de l'aLPD quant à un encadrement efficace du profilage[340].

En parallèle à ces travaux législatifs au sein du DFJP, le Département fédéral des finances (ci-après « DFF ») a institué le 27 août 2015 – en réponse à la motion RECHTSTEINER du 3 décembre 2013 (13.3841) – le groupe d'experts « Avenir du traitement et de la sécurité des données »[341] pour une durée de trois ans. Ce

336 Rapport du groupe d'accompagnement Révision LPD, pt. 4.4.6.

337 Rapport du groupe d'accompagnement Révision LPD, pt. 4.4.6.

338 Rapport du groupe d'accompagnement Révision LPD, idem.

339 Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données, pt. 1.4.1.

340 Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données, pt. 8.1.1.3.

341 Ce groupe d'experts était présidé par Mme BRIGITTA M. GADIENT, ancienne membre du Conseil national et se composait d'experts scientifiques, juridiques, économiques ainsi que de quelques membres de l'administration fédérale, pour un aperçu plus détaillé,

groupe d'experts a publié son rapport le 17 août 2018 dans lequel les experts ont, entre autres, décrit les défis posés par le développement du profilage non seulement de manière générale[342] mais aussi plus spécifiquement dans le cadre d'une procédure d'embauche[343].

À la lumière de l'aLPD et de l'avant-projet de loi, les experts estiment qu'« étant donné que ce type de traitement porte sur des traits de personnalité importants du candidat (profilage), il nécessite le consentement préalable et explicite de la personne concernée (art. 4 al. 5 aLPD). Ce consentement est cependant soumis à caution dans le monde du travail, car les procédures de recrutement et les rapports de travail n'offrent généralement pas au candidat la possibilité d'exprimer sa volonté librement, alors qu'il s'agit là d'une condition de validité du consentement »[344]. Estimant que les risques d'atteinte à la personnalité des candidats concernés sont importants, les experts arrivent à la conclusion que même la (nouvelle) LPD n'est pas en mesure de contrer ces risques. Ainsi, ils conseillent de « développer les lois spéciales correspondantes afin de les harmoniser avec le droit de la protection des données »[345].

Malgré ces divers travaux très extensifs et qui tous, de façon de plus en plus urgente, ont pu démontrer la nécessité de légiférer en la matière, la nouvelle LPD n'a que pu être adoptée le 25 septembre 2020 et n'entrera en vigueur que le 1er septembre 2023. Ce long délai est dû, entre autres, aux nombreux débats parlementaires qui ont porté sur la définition du profilage[346]. Cependant, il convient de noter que la LPD n'a pas été soumise au référendum facultatif[347] ce qui peut être interprété comme preuve qu'un compromis a su être trouvé (ou, dans une veine plus cynique, que les enjeux sont trop complexes pour facilement mobiliser la société civile).

voir Rapport d'experts concernant le traitement et la sécurité des données du 17 août 2018, Annexe 1 : Composition du groupe d'experts.

342 Rapport du groupe d'experts concernant le traitement et la sécurité des données du 17 août 2018, pt. 5.3.1.6.

343 Rapport du groupe d'experts concernant le traitement et la sécurité des données du 17 août 2018, pt. 10.2.2.

344 Rapport du groupe d'experts concernant le traitement et la sécurité des données du 17 août 2018, pt. 5.3.1.9.

345 Rapport du groupe d'experts concernant le traitement et la sécurité des données du 17 août 2018, idem.

346 Pour un résumé des débats parlementaires à ce sujet, voir Objet du Conseil fédéral 17.059, Loi sur la protection des données. Révision totale et modification d'autres lois fédérales tel que cité par MÉTILLE, voir MÉTILLE, La (nouvelle) loi fédérale, p. 2.

347 Art. 141 al. 1er let. a Cst. En effet, le délai référendaire fixé au 14 janvier 2021 s'est écoulé sans qu'un référendum n'ait été soumis à la Chancellerie fédérale.

Ainsi, tel que mentionné plus haut, l'art. 5 let. f LPD définit le profilage de la manière suivante :

> « On entend par : *profilage* (sic) : toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

Au paragraphe suivant, la LPD vient définir une forme particulière du profilage. L'art. 5 let. g LPD se lit comme suit :

> « On entend par : *profilage à risque élevé* (sic) : tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ».

Ayant conscience que certaines formes de profilage peuvent porter atteinte aux droits fondamentaux, mais que la LPD n'a, en principe, pas pour but de protéger lesdits droits fondamentaux dans les relations entre particuliers (mais uniquement leur personnalité)[348], les deux Chambres ont décidé de palier à ce problème en introduisant cette sous-catégorie de profilage. Cette spécificité suisse[349], introduite lors des derniers débats parlementaires[350], soulève toutefois plusieurs problèmes de mise en œuvre qu'il conviendra de mettre en lumière[351].

En l'absence de jurisprudence, il convient de soulever quelques points qui pourraient s'avérer problématiques lors de la mise en pratique de ces deux nouvelles définitions, notamment dans le cadre d'une procédure d'embauche.

348 Art. 1er LPD, pour une analyse plus approfondie, voir ROSENTHAL, Das neue Datenschutzgesetz, N 12 ; FASNACHT, N 9.

349 On notera que depuis novembre 2021, la Recommandation profilage 2021 prévoit également une définition des « traitements de profilage à risque élevé ». Cette définition ne correspond toutefois pas à celle prévue par le Législateur suisse, voir l'art. 1 let. j Recommandation profilage 2021.

350 Cette décision de dernière minute explique l'absence de commentaires à ce sujet dans le Message du Conseil fédéral, voir FF 2017 6565.

351 Voir *infra* Chapitre 8. de la loi sur la protection des données.

B. La nouvelle définition du profilage dans le contexte d'une procédure d'embauche

D'abord, force est de constater que le profilage est défini comme « toute forme de traitement automatisé ». Ainsi, la première question qui se pose est celle de savoir quels traitements de données doivent être considérés comme des traitements de données *automatisés* au sens de la nouvelle LPD. Le Message du Conseil fédéral précise à ce sujet qu'un « profilage se caractérise par le fait qu'on procède à une évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est *entièrement*[352] automatisé. On entend par évaluation automatisée toute évaluation fondée sur des techniques d'analyse informatisées. Le recours à des algorithmes est possible mais non-constitutif du profilage »[353]. Ainsi, il serait concevable de procéder à une évaluation *presque* entièrement automatisée de certains aspects de la personnalité afin d'éviter que le traitement envisagé ne tombe dans le champ de la définition. En d'autres termes, il est possible que le responsable du traitement contourne la définition légale en prévoyant qu'une partie (négligeable) du processus d'évaluation soit prise en charge par une personne physique (p. ex. la confirmation de l'évaluation faite par l'algorithme). En effet, en pratique, la plupart des évaluations impliqueront une intervention humaine (marginale)[354].

Ainsi, l'employeur qui souhaiterait effectuer un profilage sans toutefois que ce traitement de données ne tombe sous la définition de l'art. 5 let. f LPD pourrait effectuer une évaluation automatisée des données personnelles du candidat et prévoir, à titre d'exemple, qu'il confirme ou infirme l'évaluation faite avant de la valider, p. ex. en signant un document. Dans cette hypothèse, il serait facile d'argumenter que le recruteur avait encore une marge d'appréciation en cochant

---

352 Italique ajouté par mes soins.

353 FF 2017 6642.

354 ROSENTHAL est d'avis que « [traduction] si le Message précise qu'il n'y a profilage que si le processus d'évaluation est entièrement automatisé, il faut en conclure que si [...] la première étape du processus d'évaluation – la détermination de la note qui est encore considérée comme suffisante [pour être invité à un entretien d'embauche] – a été effectuée manuellement il n'y a donc pas de profilage [...]. Il n'est pas clair si le Conseil fédéral a voulu être aussi restrictif. Cette exigence d'une automatisation complète du processus d'évaluation ne ressort pas du texte légal, et il ne faut pas accorder beaucoup de poids au Message à ce sujet », voir ROSENTHAL, Entwurf, N 24 ; dans le sens inverse, VASELLA défend une définition stricte du critère du traitement automatisé dans le cadre d'un profilage, voir VASELLA, Entwurf, p. 2 ; à propos du droit européen (moins restrictif), voir CUSTERS/URSIC, p. 340.

(ou pas) la case prévue à cet effet à la fin de l'évaluation et que dès lors, il ne s'agissait pas d'un traitement de données automatisé *dans sa totalité*. Il va sans dire qu'en pratique, il n'est que peu probable que le recruteur se distance de l'évaluation automatisée proposée. En d'autres termes, il semble assez aisé, pour un responsable du traitement informé, de contourner la définition légale suisse. Dès lors, il convient d'attendre les décisions juridictionnelles qui auront pour mission de clarifier si la définition proposée est à entendre strictement (dès qu'une intervention humaine [même marginale] est prévue, le traitement de données ne constitue pas un profilage) ou pas. Le Message du moins laisse penser que le Législateur a entendu la définition de manière stricte[355].

Ensuite, il convient de relever que le fait que la définition n'englobe uniquement les traitements de « données personnelles » pourrait s'avérer problématique pour les personnes concernées. En effet, les courtiers en données ne traitent non seulement des données personnelles[356] mises à disposition par les personnes elles-mêmes (*voluntary personal data*) ou par des entités tierces privées ou publiques (*data created by others*), mais aussi des données anonymes (*anonymous data*)[357]. Les données anonymes ne sont pas des données personnelles au sens de la LPD[358]. Dès lors, un traitement (même automatisé) de données anonymes n'est pas soumis au régime de la LPD. Or, certains traitements automatisés de données permettent d'analyser, respectivement de prédire certains comportements individuels sur la base de données anonymes[359]. En d'autres termes, ce choix de définition implique qu'une évaluation automatisée de données *non-personnelles* (données anonymes) ne tomberait pas sous le coup de la définition du profilage quand bien même la collecte (*data warehousing*) puis l'analyse de de données (*data mining*) anonymes peuvent constituer les deux premières étapes d'un profilage (création de « profils anonymes »). De plus, la création de profils sur la base de données anonymes peut entraîner la réidentification des individus qui se cachent derrière lesdites données ano-

355 Dans le même sens, voir FÜZESSÉRY/SCHNEIDER, p. 145 ; englobant également des traitements qui ne sont pas entièrement automatisés, la définition européenne du profilage semble être plus large que la définition retenue en droit suisse, voir, pour une analyse plus approfondie, *infra* Chapitre 8. de la loi sur la protection des données.

356 On rappellera que la doctrine majoritaire s'accorde à considérer que la notion de « donnée personnelle » englobe également les données dites « pseudonymes », voir MÉTILLE, Internet et droit, p. 81 ; dans le même sens, voir HEUBERGER, N 127 s. ; pour une position moins stricte, voir MEIER, Protection des données, N 446 s.

357 BERANEK ZANON, p. 92 ; PROBST, p. 18.

358 Art. 2 al. 1er et 5 let. a LPD *a contrario* ; pour des précisions quant à la définition de « donnée personnelle » et un aperçu d'exemples tirés de la pratique, voir FF 2017 6639 s.

359 ROUVROY, pp. 20 ss. ; HEUBERGER, N 131 ss.

nymes. En effet, les développements techniques permettent de procéder à de telles ré-identifications de plus en plus facilement[360], étant précisé qu'une telle ré-identification constitue incontestablement un traitement de données personnelles soumis au régime de la LPD[361].

Il découle de ce qui précède que les deux premières étapes d'un profilage, qui peuvent, dans certains contextes, aboutir à la création d'un profil contenant des données sensibles, ne tomberait pas dans le champ de la définition du profilage. Ainsi, il est regrettable que la nouvelle définition n'englobe pas toutes les diverses étapes d'un profilage, notamment la collecte et l'analyse de données anonymes, mais seulement les traitements ultérieurs à la constitution de profils sur la base de données anonymes.

Il est intéressant de relever que la définition du profilage retenue dans l'avant-projet de LPD ne prévoyait pas que l'information traitée de manière automatisée consiste en une donnée personnelle[362] et aurait donc permis une application plus large de la définition du profilage[363]. Il semble que la définition du profilage n'encadre que partiellement ce nouveau traitement de données et engendre ainsi une insécurité juridique supplémentaire dans la mesure où, en pratique, il peut se révéler hasardeux de déterminer à partir de quel moment la LPD vient à s'appliquer[364].

360 À titre d'exemple, un groupe de chercheurs a collecté, une fois par heure pendant 15 mois, les données d'emplacement anonymes de 1.5 million d'individus. Grâce à des calculs statistiques, quatre points spatio-temporels suffisaient afin d'identifier de façon unique 95 % des individus, voir MONTJOYE et al., pp. 1 ss. Un tel procédé constitue un traitement automatisé, qui se fonde sur des données anonymes, donc des données non-personnelles au sens de la LPD, mais qui peut (mais ne doit pas nécessairement) aboutir à une analyse très précise des habitudes des personnes concernées comportant potentiellement des données sensibles (p. ex. si une coordonnée a été relevée dans une clinique proposant des avortements ou un lieu de culte) ; pour un exemple similaire évoquant l'exploitation d'une base de données anonymisées d'une banque contenant trois mois de transactions effectuées par carte de crédit dans le but de ré-identifier les détenteurs desdites cartes de crédit et de nombreuses références juridiques supplémentaires au sujet de la difficulté de garantir l'anonymat de données au temps du *Big Data*, voir MEIER, Big Data, p. 56 ; pour un reportage récent à propos de cette thématique aux États-Unis, voir THOMPSON/WARZEL, Twelve Million Phones, One Dataset, Zero Privacy.

361 BERANEK ZANON, p. 92.

362 L'avant-projet de LPD prévoyait en effet que « le profilage se définit [...] comme toute exploitation de données, personnelles ou non, qui consiste à analyser ou prédire les caractéristiques personnelles essentielles d'une personne » pour préciser, quelques lignes plus loin que « la définition légale englobe l'exploitation de données personnelles et non personnelles et tient ainsi compte du fait qu'avec les technologies actuelles (Big Data), l'analyse de données sans lien avec une personne fasse émerger des données personnelles », voir Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données, pt. 8.1.1.3.

363 CELLINA, Le profilage, p. 2.

364 À juste titre, même avant tout projet de révision de la LPD, voir PROBST, p. 33 et MEIER, Big Data, pp. 57 s.

De plus, le but du profilage est défini comme l'évaluation de « certains aspects personnels relatifs à une personne physique ». La définition extensive du but du profilage est à saluer dans la mesure où le profilage peut être utilisé dans des contextes très divers[365]. Toutefois, ce troisième élément de la définition du profilage ainsi défini soulève la question de savoir quels aspects personnels peuvent être évalués dans le cadre d'un profilage sans pour autant tomber sous le coup de la définition légale et lesquels, au contraire, seront soumis au régime prévu par la LPD. Dans ce contexte, il est regrettable que le Message ne cite que quelques exemples et reste vague sur le but d'un profilage effectué. Ainsi, le Message fixe, de manière générale, que le profilage peut être utilisé pour « analyser ou prédire [le] rendement au travail, [la] situation économique, [la] localisation, [la] santé, [le] comportement, [les] préférences ou [les] déplacements [de la personne concernée] » avant de ne citer qu'un seul exemple : « L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité »[366]. Ceci est d'autant plus regrettable que le profilage permet d'évaluer de multiples aspects de la personnalité d'un individu. À titre d'exemple, l'utilisation d'un certain navigateur lors de la soumission d'un dossier de candidature a été utilisée pour évaluer le rendement potentiel au travail, le nombre de réseaux sociaux gérés par une même personne physique a contribué à déterminer s'il valait la peine de l'engager à l'heure, les mouvements effectués durant la journée de travail ou la tonalité de la voix enregistrée puis évaluée par un microphone portable allumé en permanence ont conduit à l'évaluation de la personnalité d'employés[367]. Est-ce que l'analyse du navigateur utilisé pour la soumission du dossier de candidature constituerait déjà un traitement de données automatisé mis en place afin d'évaluer *certains aspects personnels* de la personne candidate ? Est-ce que l'évaluation du nombre de réseaux sociaux utilisés par un candidat pourrait être qualifiée d'évaluation de *certains aspects de la personnalité* dudit candidat ? Au regard et de la définition légale et du Message, la réponse à ces questions ne semble pas être évidente. Cette constatation conduit à une insécurité supplémentaire pour un employeur qui souhaiterait effectuer un profilage d'un candidat.

En outre, la distinction entre un profilage « général » et un « profilage à risque élevé » est problématique pour plusieurs raisons. D'abord, dans la mesure où la notion de « risque élevé » est une notion floue, elle devra, sans nul

365 Voir *supra* Chapitre 3. Exemples de profilage dans différents secteurs d'activités.

366 FF 2017 6642.

367 CHRISTL/SPIEKERMANN, pp. 32 ss.

doute, être précisée par les tribunaux[368]. Jusque-là, il n'est que peu clair quels traitements de données devraient être qualifiés de profilage « général » (évaluation d'aspects personnels) et lesquels, au contraire, de « profilage à risque élevé » (appréciation des caractéristiques essentielles). Une lecture littérale de la définition semble toutefois laisser entendre qu'un profilage portant une simple atteinte à un droit fondamental n'est pas suffisant pour tomber sous le coup de la définition de « profilage à risque élevé ». En introduisant cette distinction lors de la session d'hiver 2019, le Conseil aux États n'a, partiellement du moins, pas su atteindre un des buts de la révision de la LPD : l'amélioration de la sécurité juridique lors de l'utilisation de nouvelles technologies[369]. En effet, cette distinction a été introduite après la publication du Message ce qui implique que le Message ne contient aucune précision quant à la mise en œuvre de cette distinction.

En outre, rien n'empêche un particulier, comme p. ex. un employeur, d'effectuer un profilage qui porte atteinte à certains intérêts protégés par les droits fondamentaux[370]. D'un point de vue abstrait, il est donc concevable qu'un employeur puisse procéder à un profilage à risque élevé. L'introduction de cette définition peut ainsi faire croire que le Législateur entendait conférer un effet horizontal direct aux droits fondamentaux, notamment lorsqu'un profilage représente un risque élevé d'atteinte auxdits droits. Or, à la lecture des passages du Message consacrés à d'autres dispositions introduites dans la nLPD, qui mentionnent également les droits fondamentaux (art. 7 al. 2 LPD et 22 al. 1er LPD), il ressort que la LPD a pour but de protéger les droits fondamentaux uniquement lorsque les traitements sont effectués par des organes fédéraux. Entre particuliers, la LPD a vocation à protéger la personnalité des personnes concernées[371]. Si la doctrine semble exclure un quelconque effet horizontal direct des droits fondamentaux par le biais de la LPD, l'introduction de la définition du profilage à risque élevé à la toute fin des débats parlementaires, c'est-à-dire bien après la rédaction du Message, permet de se demander si l'exclusion d'un

368 Constatation du Prof. THOUVENIN, mise en avant dans le cadre de son cours « Informations- und Kommunikationsrecht » au semestre d'automne 2020 à l'Université de Zurich, voir THOUVENIN, Informations- und Kommunikationsrecht, p. 14 ; Les précisions de cette notion viendront éventuellement du Conseil de l'Europe dans la mesure où le Comité des Ministres a introduit cette notion dans la Recommandation profilage révisée en 2021. On notera toutefois que la « définition » du Comité des Ministres est formulée bien différemment que celle fixée en droit suisse dans la mesure où elle contient une énumération d'exemples (non-exhaustive) de profilages à risque élevé sans toutefois offrir une définition générale et abstraite de ce traitement de données, voir *supra* Chapitre 2. La définition compliquée du profilage.

369 FF 2017 6592.

370 Voir *supra* Méthodologie.

371 FF 2017 6649 ; repris par ROSENTHAL, Das neue Datenschutzgesetz, N 15 et KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, pp. 43 s.

quelconque effet horizontal direct des droits fondamentaux dans le contexte du profilage correspond en effet à la volonté du Législateur et est judicieuse. Au vu des risques d'un profilage effectué pendant la procédure d'embauche on peut se demander si l'effet horizontal direct des droits fondamentaux doit également être catégoriquement exclu. Seuls les tribunaux pourront répondre à cette question. L'introduction de cette distinction à la dernière minute n'a vraisemblablement pas apporté une réponse claire aux nouveaux défis, mais soulève, bien au contraire, de nombreuses nouvelles incertitudes.

Afin de remédier à l'insécurité juridique qui entoure la notion de « profilage à risque élevé », certains auteurs ont non seulement proposé d'exclure un quelconque effet horizontal des droits fondamentaux en présence d'un tel profilage, mais ont également suggéré que le « risque élevé » tel que mentionné à l'art. 5 let. g LPD soit entendu de la même manière que le risque élevé déterminé dans le cadre d'une analyse d'impact (art. 22 LPD)[372]. En d'autres termes, ils proposent l'approche suivante : en principe, un responsable du traitement peut effectuer un profilage, qui conduit à la création d'une image complète d'une personne ou de ses caractéristiques essentielles. Dans un deuxième temps, le responsable doit procéder à une analyse d'impact. Dans le cadre de cette analyse, il devra se demander si le traitement envisagé risque d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Si la réponse à cette question est affirmative, il lui incombera, dans un troisième temps, de mettre en œuvre des mesures qui atténueront les risques identifiés. Si même après la mise en œuvre de ces mesures, le risque reste élevé, le responsable devra consulter le PFPDT qui disposera ensuite d'un délai de deux mois pour prendre position. Le responsable peut exceptionnellement renoncer à une analyse d'impact (exception qui sera probablement souvent invoquée en pratique) s'il remplit l'une des conditions fixées à l'art. 22 al. 4 ou 5 LPD[373].

Une telle lecture conduit toutefois à un inconvénient non-négligeable : Elle implique que certains profilages, qui aboutissent à l'obtention d'une telle image complète d'une personne concernée sont licites et n'impliquent pas la

372 ROSENTHAL, Das neue Datenschutzgesetz, N 27 ; position reprise par Me JÜRG SCHNEIDER dans sa présentation intitulée « Nouvelles définitions et nouveaux motifs justificatifs » qui a eu lieu dans le cadre de la Journée de droit de la protection des données le 9 mars 2021 à l'Université de Lausanne.

373 D'une part, une analyse d'impact n'est pas obligatoire lorsque le responsable du traitement privé est tenu d'effectuer le traitement en vertu d'une obligation légale. D'autre part, le responsable du traitement peut renoncer à une telle analyse s'il recourt à un traitement de données certifié ou qu'il respecte un code de conduite tel que défini à l'art. 11 LPD ; pour une analyse critique de l'efficacité des certifications et des codes de conduite, voir *infra* Chapitre 8. La Loi sur la protection des données.

mise en place de mesures supplémentaires, comme p. ex. une analyse d'impact *complète*. Or, une telle lecture est contraire à la volonté du Législateur. En effet, la définition du profilage à risque élevé a été introduite à la dernière minute par le Législateur qui considérait que le fait de procéder à un appariement (automatisé) de données ayant pour conséquence de rendre la personne concernée transparente entraînait un risque élevé[374]. En d'autres termes, le Législateur n'entendait à aucun moment fixer que les profilages conduisant à la création automatisée de profils de la personnalité tels que définis à l'art. 3 let. d aLPD étaient, en principe, licites[375] et n'étaient dès lors que ponctuellement soumis à une analyse d'impact.

Il découle de ce qui précède que si la lecture uniforme de la notion de « risque élevé » proposée par ROSENTHAL a certes l'avantage d'alléger les obligations incombant aux entreprises privées, elle semble être contraire au but de la révision de la LPD. Les Parlementaires ont introduit cette distinction – certes malencontreusement formulée – afin d'encadrer les utilisations problématiques du profilage. Un alignement du contenu du « risque élevé » tel que prévu à l'art. 5 let. g LPD sur celui mentionné à l'art. 22 LPD ne semble dès lors pas correspondre à la volonté du Législateur ; l'utilisation de la même notion dans les deux dispositions ne devrait pas être interprétée comme volontaire, mais, bien au contraire, comme une maladresse rédactionnelle de dernière minute.

Il est à espérer que les tribunaux compétents éclairciront rapidement cette question de manière contraignante, p. ex. en s'inspirant des travaux récents du Conseil de l'Europe[376]. L'employeur qui souhaiterait recourir au profilage se

374 On notera que la définition du « profilage » telle que consacrée à l'art. 5 let. f LPD ne comprend pas l'élément de l'« appariement ».

375 On rappellera que le Message relatif à l'aLPD précisait que par « profil de la personnalité on entend un assemblage de données relatives aux traits de la personnalité, aux compétences professionnelles ou aux activités extra-professionnelles, assemblage susceptible de donner une image complète d'une personne ou de ses caractéristiques essentielles », voir FF 1988 454. En d'autres termes, ROSENTHAL a raison en affirmant que l'introduction de la définition de « profilage à risque élevé » a conduit à réintroduire le « profil de la personnalité » connu sous le régime de l'aLPD, ROSENTHAL, Das neue Datenschutzgesetz, N 27 ; dans ce contexte, on relèvera la modification d'ordre formel relative au remplacement du terme d'« assemblage » par celui d'« appariement ».

376 Pour une analyse de la nouvelle définition du profilage à risque élevé proposée par le Comité des Ministres dans la Recommandation profilage 2021, voir *infra* Chapitre 12. Le cadre prévu par le Conseil de l'Europe ; s'il est vrai que l'art. 1er al. 2 et 3 OPDo apporte quelques précisions quant à l'évaluation du risque lors de la mise en place de mesures visant à garantir la sécurité des données (principe de sécurité des données), force est de constater que les critères mentionnés sont vagues et que le rapport y relatif n'apporte que peu de précisions quant à ce qui doit être entendu par « risque élevé » (à la lumière du principe de sécurité), voir OFJ, Rapport explicatif sur la révision de l'ordonnance sur la protection des données du 31 août 2022, pp. 20 s.

voit, une fois de plus, confronté à une insécurité juridique. Un employeur qui voudrait s'assurer du bon respect du cadre légal partira alors très probablement du principe que tout profilage sur le lieu de travail constitue un profilage à risque élevé. Il va sans dire qu'une telle évolution en pratique ne devrait pas non plus correspondre à la volonté du Législateur, qui ne souhaitait pas inutilement alourdir les obligations légales des responsables de traitement[377].

De surcroît, savoir comment articuler un recours cumulatif au profilage tel que défini à l'art. 5 let. f et g LPD d'une part et à une décision automatisée telle que définie à l'art. 21 LPD d'autre part, n'a pas été tranché par la LPD[378]. En effet, l'art. 21 LPD prévoit que « le responsable du traitement informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative (décision individuelle automatisée) ». À la lumière de cette disposition, les conditions en vertu desquelles le traitement de données litigieux doit être « uniquement » qualifié de profilage et celles qui permettraient, en revanche, de qualifier un traitement de données automatisé comme « affectant la personne concernée de manière significative » devront être précisées. Cette insécurité juridique est avant tout liée à la question de ce qui doit être entendu par la notion de « décision qui affecte la personne concernée de manière significative » d'une part et « évaluation de certains aspects de la personnalité » d'autre part. Il est concevable qu'un profilage puisse, dans certaines hypothèses, affecter la personne concernée de manière significative et être perçu davantage comme une décision qu'une « simple » évaluation. Cette constatation risque d'être plus vraie encore si le responsable du traitement s'aligne, lors de la prise de décision, sur l'évaluation automatisée.

Dans l'hypothèse où un traitement de données automatisé est qualifié de décision ayant « un effet significatif » sur la personne concernée, un régime juridique plus lourd s'applique (devoir d'informer etc.). Ici encore, une insécurité juridique a été créée par les rédacteurs de la LPD. Toutefois, même si le régime plus lourd tel que prévu à l'art. 21 LPD venait à s'appliquer, sa portée dans le cadre d'une procédure d'embauche semble être limitée. En effet, l'art. 21 al. 3 let. a LPD prévoit que si « la décision individuelle automatisée est en relation directe avec la conclusion [...] d'un contrat entre le responsable du traitement et la personne concernée et [que] la demande de cette dernière est satisfaite » le devoir d'informer qui, en principe, incombe au responsable du traitement, tombe. Ainsi, si une personne a été embauchée sur la base d'une décision

377 FF 2017 6596.

378 Dans le même sens et avec quelques pistes quant à de possibles critères de distinction, voir HEUBERGER, N 186 ss.

individuelle automatisée (demande satisfaite), elle perd son droit à être informée de cette décision, de faire valoir son point de vue et à une nouvelle évaluation par une personne physique. Si, au contraire, le candidat n'est pas retenu, il pourra faire valoir ses droits tels que consacrés à l'art. 21 al. 1er et 2 LPD. La nature de ces droits reste toutefois peu claire et ils ne semblent être que peu efficaces en pratique[379].

Enfin, la décision du Parlement suisse d'explicitement mentionner l'utilisation du profilage dans le contexte du travail dans la LPD est à saluer. Cependant, il est regrettable qu'une notion plus précise que « rendement au travail » n'ait pas été choisie pour décrire le but d'un profilage effectué dans ce contexte[380]. En effet, dans le cadre spécifique du recours au profilage lors d'une procédure d'embauche on peut se demander ce que la notion de « rendement au travail » recouvre. Dans le contexte du travail, cette notion décrit l'efficacité de quelqu'un dans son travail et est ainsi synonyme d'« efficience » ou de « productivité »[381]. Sur la base d'une interprétation littérale, la LPD ne viendrait donc qu'encadrer les cas dans lesquels le traitement de données automatisé viendrait évaluer et potentiellement prédire si le candidat est une personne efficace. Or, comme nous l'avons vu plus haut, il est possible, entretemps, de calculer la probabilité de certains comportements sur le lieu de travail allant bien au-delà du simple « rendement ». Ainsi, l'utilisation du profilage permet de calculer la probabilité avec laquelle une certaine personne a un esprit d'équipe ou si un candidat a des opinions prononcées par rapport à certaines questions de nature politique ou religieuse. Dans ces cas de figure, qui renvoient potentiellement à un traitement de données sensibles, il ne s'agit pas de traitements de données personnelles portant sur le rendement à proprement parler. Dès lors, dans le but de garantir la protection de la personnalité et le respect des droits fondamentaux de toute personne se portant candidate à un poste en Suisse, j'estime qu'il convient, à défaut de jurisprudence ou d'une révision prochaine, d'adopter une lecture extensive de la notion de « rendement au travail ». En d'autres termes, il convient d'englober, dans cette notion, toutes les formes d'évaluations automatisées de la personnalité des candidats. Une telle lecture généreuse est d'ailleurs corroborée par le fait que la liste d'exemples cités à l'art. 5 let. f LPD est non-exhaustive.

Il découle donc de ce qui précède :

— que la définition choisie du profilage n'englobe potentiellement pas tous les cas dans lesquels un tel traitement de données est effectué, notamment

379 Voir *infra* Chapitre 8. La Loi sur la protection des données.

380 Cette notion a été reprise de l'art. 4 ch. 4 RGPD.

381 Dictionnaire Larousse, Rendement, nom masculin.

lorsque l'évaluation finale de la personnalité d'un candidat est validée par un être humain (qui peut tout simplement confirmer ce que le traitement automatisé a suggéré) ;

— que le but du profilage tel qu'envisagé par la loi n'est pas l'unique but potentiellement recherché par les employeurs utilisant le profilage lorsqu'ils doivent évaluer différents candidats ;
— que la distinction introduite entre le « profilage » et le « profilage à risque élevé » crée une insécurité juridique non-négligeable et ne semble pas contribuer à une meilleure protection des droits fondamentaux des personnes concernées dans toutes les hypothèses identifiées.

La plus grande difficulté juridique réside toutefois dans le fait que la nouvelle LPD a certes introduit deux définitions du profilage, mais – même après avoir reconnu les potentiels risques posés aux droits des personnes concernées – ne soumet pas ce nouveau traitement de données à un régime spécial, respectivement renforcé[382]. Ainsi, le Législateur a fait le choix de ne pas encadrer ce traitement de données potentiellement à hauts risques autrement que par les principes généraux.

Lorsqu'un employeur soumet des candidats à un profilage, il doit non seulement se demander si le traitement choisi peut être qualifié de profilage, voire de profilage à risque élevé, mais aussi (et surtout) veiller à adhérer aux principes généraux, qui sont consacrés par la LPD.

C. Le profilage pendant la procédure d'embauche à la lumière des principes généraux

Comme nous l'avons vu plus haut, et l'aLPD et la LPD ont pour but de protéger la personnalité des personnes physiques. Ainsi, une des questions centrales du droit de la protection des données est celle de savoir quels traitements de données personnelles portent atteinte à la personnalité des personnes concernées. L'art. 30 LPD prévoit qu'il y a atteinte illicite à la personnalité lorsqu'un des principes généraux prévus aux art. 6 et 8 LPD a été violé (art. 30 al. 2 let. a LPD), lorsque des données sont traitées contre la volonté expresse de la personne concernée (art. 30 al. 2 let. b LPD) ou lorsque des données sensibles sont communiquées à des tiers (art. 30 al. 2 let. c LPD). Toutefois, il convient de noter que

382 La seule exception figure à l'art. 6 al. 7 let. b LPD qui prévoit qu'il ne peut être procédé à un profilage à risque élevé si la personne concernée n'a pas donné son consentement exprès ; cette exception devrait toutefois n'avoir qu'une portée très marginale en pratique, pour plus de développements relatifs au consentement exprès, voir *infra* Chapitre 8. La Loi sur la protection des données.

cette liste n'est pas exhaustive[383]. En d'autres termes, une violation de la personnalité est présumée lorsque l'employeur viole un des principes généraux, lorsque le candidat a expressément fait valoir sa volonté que le profilage envisagé ne soit pas effectué ou lorsque l'employeur transmet des données sensibles, relatives au candidat, à des tiers.

Inversement, le régime prévu à l'art. 30 LPD implique que si un traitement de données est conforme aux principes généraux, il n'y a pas violation de la personnalité. Aucun motif justifiant le traitement de données ne devra alors être avancé par le responsable du traitement. Sur ce point, le droit suisse va moins loin que le RGPD qui fixe que tout traitement de données porte, en principe, atteinte à la personnalité de la personne concernée (principe du *opt-in*). Dès lors, tout traitement de données personnelles doit être justifié en droit de l'UE[384]. La Convention 108 quant à elle prévoit un régime similaire à celui prévu en droit européen[385].

Ainsi, en droit suisse, on peut se demander si une atteinte est illicite au sens de l'art. 30 LPD[386]. Dès lors, après avoir analysé les deux nouvelles définitions du profilage, il convient de se demander si un profilage tel que défini dans la

383 FF 2017 6688.

384 Art. 6 RGPD. FÜZESSÉRY et SCHNEIDER estiment toutefois que cette différence de régime est plus théorique que pratique étant donné que « s'il est vrai que la conception du Législateur fédéral est un peu plus libérale que celle du Législateur européen, les deux systèmes aboutissent à des résultats semblables puisque les motifs de licéité sont comparables », voir FÜZESSÉRY/SCHNEIDER, p. 153. Reste à savoir si l'UE partagera cette analyse dans le cadre du renouvellement de la décision d'adéquation de la Suisse. Si MÖHLE relève également cette différence de régime et qu'il laisse ouvert si le principe du *opt-out* offre une protection adéquate des droits des personnes concernées, il semble être d'avis que c'est avant tout le manque d'indépendance du PFPDT qui pourrait (négativement) impacter la décision d'adéquation de l'UE, pour plus de détails quant aux critères potentiellement pris en compte dans le cadre de cette décision, voir MÖHLE, pp. 599 ss.

385 Art. 5 al. 2 Convention 108+.

386 Sous le régime de l'aLPD, savoir si la violation d'un principe général entraînait automatiquement une atteinte illicite à la personnalité ou si une telle violation pouvait être justifiée avait généré des incertitudes dans les milieux professionnels. L'OFJ, conscient que cette incertitude juridique pouvait poser des problèmes en pratique et que le Tribunal fédéral n'avait pas été appelé à trancher cette question, avait publié un guide non-contraignant afin de clarifier qu'un traitement de données contraire à un principe général pouvait être justifié et ainsi être rendu licite au sens de l'aLPD. On rappellera toutefois l'exception à cette règle : une violation du principe de la bonne foi ne pouvait être justifiée, voir OFJ, Modification de l'art. 12 al. 2 let. a LPD : Notice interprétative, janvier 2007. La révision de la LPD a apporté une réponse définitive à cette question en modifiant l'art. 12 al. 2 let. c aLPD. Désormais, il ressort clairement du texte légal qu'une atteinte à la personnalité illicite telle que définie à l'art. 30 LPD peut être justifiée par un des motifs justificatifs prévus à l'art. 31 al. 1er LPD.

LPD effectué dans le contexte d'une procédure d'embauche serait contraire à l'un des principes généraux tels que fixés aux art. 6 LPD (1-4), 8 LPD (5) et 30 al. 2 let. b et let. c LPD (6-7).

1. Le principe de la bonne foi (art. 6 al. 2 LPD)

À titre préliminaire, il convient de noter que cette disposition n'a pas subi de modifications formelles ou matérielles dans le cadre de la révision. Le Message du Conseil fédéral ne prend pas même position par rapport au principe de la bonne foi[387]. Ainsi, on rappellera que contrairement aux autres principes généraux dont la violation peut être justifiée par un des motifs justificatifs fixés par la LPD, il n'est pas envisageable de contourner le principe de la bonne foi[388].

Comme mentionné en amont, le Tribunal fédéral n'a pas été amené à se prononcer à propos du cadre juridique à donner au profilage sous le régime de l'aLPD. À plus forte raison, il n'a jamais été amené à rechercher si un profilage dans le cadre d'une procédure d'embauche était contraire au principe général de la bonne foi ou pas. Toutefois, quelques auteurs se sont penchés sur la question plus générale de savoir dans quelles hypothèses un employeur pourrait porter atteinte au principe de la bonne foi. STAEHELIN considère que l'employeur qui procéderait à un traitement de données personnelles de l'employé par hasard ou pour d'autres raisons que pour celles pour lesquelles l'employé a donné son consentement[389], violerait le principe de la bonne foi au sens de l'art. 12 aLPD[390]. ROSENTHAL quant à lui estime que le principe de la bonne foi est une clause générale du droit de la protection des données qui s'applique lorsque les (autres) principes généraux n'encadrent pas le traitement de données ou que leur application conduit à des résultats insatisfaisants pour la personne concernée. Ainsi, avant l'introduction du principe de transparence, le fait de collecter des données à l'insu de la personne concernée (*heimliche Datenbeschaffung)* était considéré contraire au principe de la bonne foi bien que

387 FF 2017 6644 ss.

388 OFJ, Modification de l'art. 12 al. 2 let. a LPD : Notice interprétative, janvier 2007, p. 2.

389 Par rapport à la validité du consentement du candidat, voir *infra* Chapitre 8. La Loi sur la protection des données.

390 Même s'il est vrai que la prise de position de STAEHELIN ne porte seulement sur les traitements de données effectués *pendant* la relation de travail, il n'est que difficilement concevable de limiter l'argumentation de cet auteur aux relations de travail déjà entamées. En effet, à la lumière de la lettre de l'art. 328b CO qui encadre, en une phrase, les traitements de données licites dans le cadre d'une procédure d'embauche ainsi que pendant la relation de travail, adopter une approche fondamentalement différente face à ces traitements de données différés dans le temps ne semble pas être justifiée, voir STAEHELIN, art. 328b CO, N 8.

cette collecte secrète ne violait aucun (autre) principe général[391]. EPINEY quant à elle est d’avis que l’utilisation de données personnelles même librement accessibles à des fins publicitaires, notamment si la personne concernée s’y est opposé, serait contraire au principe de la bonne foi. De plus, elle précise que ce principe général implique, en principe, que le responsable du traitement collecte les données personnelles auprès des personnes concernées[392]. Pour sa part, MEIER estime que « dans une conception traditionnelle [du principe de la bonne foi], l’internaute ou le client ne doit pas s’attendre à ce que ses données soient conservées au-delà de ce qui est nécessaire à un usage raisonnable pour être mises à profit et le cas échéant partagées avec des tiers afin d’atteindre des objectifs non encore déterminés au moment de la collecte »[393]. Ces prises de position devraient toujours être valables sous le régime de la LPD révisée dans la mesure où la disposition consacrant le principe de la bonne foi n’a subi aucune modification.

Le profilage dans le cadre d’une procédure d’embauche est un traitement de données effectué très souvent (mais pas toujours) à l’insu de la personne concernée[394]. En effet, la plupart du temps, le profilage est un traitement de données « doublement secret ». Souvent, il est mis en place sans que la personne concernée en soit informée. Même dans l’hypothèse où la personne concernée aurait été informée, le raisonnement qui sous-tend l’évaluation automatisée est souvent incompréhensible (et pour la personne concernée et pour l’employeur) et a donc une nature secrète[395]. Reprenant la ligne d’argumentation de STAEHELIN et ROSENTHAL, le profilage au stade de la procédure d’embauche – à condition qu’il se fasse à l’insu du candidat – pourrait ainsi être considéré contraire au principe de la bonne foi. De plus, on rappellera que la plupart des profilages sont effectués sur la base de données collectées non pas auprès des candidats, mais auprès de tiers ou sur la base de données librement accessibles sans que l’employeur ou son sous-traitant ne se soucie de savoir si le candidat concerné s’est opposé ou non à la réutilisation de ses données. À la lumière du raisonnement

391 ROSENTHAL, art. 4 LPD, N 14.

392 EPINEY, § 9, N 22 ; pour un exemple allant dans le même sens et considéré contraire au principe de la bonne foi en droit européen, voir Groupe de travail « Article 29 » sur la protection des données, Lignes directrices relatives à la décision individuelle automatisée et au profilage, p. 11.

393 MEIER, Big Data, p. 65.

394 Voir *supra* Chapitre 5. Avantages et risques.

395 Pour les raisons pour lesquelles le raisonnement qui sous-tend le profilage est souvent difficilement compréhensible, voir *supra* Chapitre 2. La définition compliquée du profilage.

d'EPINEY et de MEIER, le profilage effectué tel que défini dans cette contribution violerait le principe de la bonne foi. Un profilage peut aboutir à des résultats insatisfaisants pour la personne concernée sans être encadré par un principe général autre que celui de la bonne foi[396]. En bref, on retiendra que le profilage au stade de la procédure d'embauche peut donc porter atteinte à la personnalité des candidats.

Vu que la LPD a uniquement vocation à protéger le droit de la personnalité et non les droits fondamentaux entre personnes privées[397], le principe de la bonne foi pourrait avoir une portée plus importante qu'en droit de l'UE[398], notamment dans toutes les hypothèses où l'application des principes généraux conduit à des résultats insatisfaisants pour les personnes concernées. Au-delà des exemples cités ci-dessus, tel sera potentiellement le cas lorsqu'un employeur procède à un profilage qui porte atteinte à un ou plusieurs intérêts protégés par les droits fondamentaux des candidats.

2. Le principe de proportionnalité (art. 6 al. 2 LPD)

En vertu du principe de proportionnalité tel que fixé à l'art. 6 al. 2 LPD, tout traitement de données personnelles doit être apte, nécessaire et raisonnable afin d'atteindre le but déterminé[399]. On notera que le but déterminé devra

396 Pour un avis moins critique, voir ROSENTHAL, Das neue Datenschutzgsetz, N 28 ; voir *supra* Chapitre 5. Avantages et risques.

397 FF 2017 6649 ; ROSENTHAL, Das neue Datenschutzgesetz, N 12 ; KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, pp. 43 s. ; une exception pourrait éventuellement être admise quant au profilage à risque élevé, voir *supra* Méthodologie.

398 REIMER, art. 5 al. 1er let. a RGPD, N 14.

399 MEIER précise que « selon la doctrine [ce principe] comprend trois composantes : la proportionnalité de principe (la nécessité du traitement doit être effective, et non seulement théorique ou éloignée), qui peut aussi s'exprimer par l'idée d'un évitement de données (*Datenvermeidung*), la proportionnalité matérielle (s'agissant en particulier de l'étendue des données collectées, conservées et traitées, qui doivent être limitées au but actuel et concret du traitement), avec une idée de minimisation des données (*Datensparsamkeit*), et enfin la proportionnalité temporelle, qui commande d'effacer ou d'anonymiser les données dès qu'elles ne sont plus nécessaires à la réalisation de la tâche pour laquelle elles ont été collectées », voir MEIER, Big Data, p. 60. S'il est vrai que cette déclinaison du principe de proportionnalité est préconisée par une partie de la doctrine, on notera que les trois composantes mentionnées par MEIER renvoient au critère de la nécessité. HEUBERGER quant à lui considère que la composante que MEIER nomme « proportionnalité matérielle » est une composante du principe de finalité, voir HEUBERGER, N 240. Afin de simplifier l'analyse qui suit, l'analyse classique, en trois temps, du principe de proportionnalité est privilégiée dans cette contribution, voir, dans le même sens, EPINEY, § 9, N 24 et 27, MEIER, Protection des données, N 665 (à propos du principe en général et non spécifiquement à propos des traitements effectués sur la base du *Big Data*) et HEUBERGER, N 233 (spécifiquement à propos du profilage).

impérativement être licite[400]. Un profilage effectué dans le cadre d'une procédure d'embauche aura pour but de s'assurer que le meilleur candidat soit sélectionné tout en économisant des ressources personnelles.

Le critère de l'aptitude d'un traitement de données oblige à se demander si le traitement choisi permet en effet d'atteindre le but fixé par le responsable du traitement. Il peut s'avérer compliqué d'admettre qu'un profilage est en effet apte à recruter le meilleur candidat dans la mesure où le profilage se fonde toujours sur des opérations arithmétiques qui ont pour but de prédire certaines probabilités et non des résultats univoques. On rappellera également que les sources d'erreurs sont multiples[401]. Ainsi, on peut se demander si la prédiction d'une probabilité devrait être considérée comme un traitement de données apte au sens de la LPD.

Dans ce contexte, on précisera que même dans le cadre d'une « procédure d'embauche traditionnelle », c'est-à-dire une procédure d'embauche menée sans recours à des nouveaux traitements de données, le recruteur fonde son évaluation du candidat sur une estimation probabiliste : souvent (mais pas toujours), une personne ayant étudié dans une université prestigieuse sera plus compétente qu'une autre personne candidate ayant étudié dans une université de faible renommée et ayant redoublé tous ses examens. Cependant, un bon recruteur est conscient que ces difficultés peuvent également être dues à des causes que le candidat n'était pas en mesure d'influencer, comme p. ex. une maladie grave survenue pendant les études ou des problèmes financiers importants, et que le candidat en question est tout aussi « apte » à pourvoir le poste que les autres candidats ayant effectué leurs études dans une université de renom et en un temps record. Le souci d'engager les « meilleurs » candidats se fonde sur une évaluation probabiliste (et qui est, de surcroît, fortement influencée par le parcours du recruteur[402]). Dans la continuation de cette argumentation, un profilage des divers candidats ne serait donc pas nécessairement moins apte à évaluer les candidats qu'une évaluation effectuée dans le cadre d'une

400 À juste titre, EPINEY rappelle que « [traduction] les particuliers sont également tenus de respecter le principe de proportionnalité. Le fait que le principe de proportionnalité soit, en principe, adapté aux traitements de données effectués par les organes publics et qu'il ait été développé à l'origine pour limiter les interventions desdits organes, entraîne la question de l'attribution d'une autre portée à ce principe lorsqu'il s'agit de traitements effectués par des particuliers. En conclusion, il convient de répondre par la négative à cette question », voir EPINEY, § 9, N 26 avec de plus amples développements quant à cette question.

401 Voir *supra* Chapitre 5. Avantages et risques.

402 À titre d'exemple, on consultera les explications d'IRIS BOHNET, voir ALEXANDER, Harvard-Professorin : « Bewerbungsgespräche sind das schlechteste Instrument, um gute Mitarbeiter*innen zu finden ».

« procédure d'embauche traditionnelle ». Cela étant, force est de constater que le profilage est souvent effectué par un *data broker*, qui évaluera les candidats sur la base de catégories de personnalité standardisées, potentiellement mal déterminées et sans tenir compte du contexte individuel[403]. Ainsi, l'évaluation de la personnalité des différents candidats risque d'être plus probabiliste encore que celle mise en place dans le cadre d'une procédure d'embauche menée directement par l'employeur qui connaît au plus près les tâches qui incomberont au nouvel employé.

Le critère de la nécessité d'un traitement de données renvoie à la question de savoir si le traitement choisi est en effet nécessaire afin d'atteindre le but déterminé par le responsable du traitement. En d'autres termes, il incombe au responsable du traitement de se demander s'il n'existe pas un autre traitement qui permettrait tout autant d'atteindre le but déterminé, mais qui porterait moins atteinte à la personnalité de la personne concernée[404]. En droit de la protection des données, le critère de la nécessité impose un « évitement de données » (*Datenvermeidung*), voire une minimisation des données (*Datensparsamkeit*) et l'obligation d'effacer ou d'anonymiser les données dès qu'elles ne sont plus nécessaires à la réalisation de la tâche pour laquelle elles ont été collectées[405].

Au vu des informations imprécises, voire délibérément fausses figurant dans de nombreux dossiers de candidature[406], il peut s'avérer nécessaire de s'assurer que les informations soumises par le candidat sont correctes. En vertu du critère de nécessité, l'employeur doit toutefois être en mesure de démontrer qu'aucune autre mesure moins intrusive n'a permis d'atteindre le but déterminé, c'est-à-dire, dans le cas d'espèce, opérer le choix du meilleur candidat grâce à des informations véridiques. À titre d'exemple, l'obligation d'indiquer le nom de jeune fille de la maman du candidat ainsi que toutes les adresses auxquelles le candidat a vécu au cours des cinq dernières années semble aller au-delà de ce qui est nécessaire à vérifier la véracité des informations soumises[407]. Dans certains cas de figure du moins, il sera sans doute moins intrusif et tout

403 Pour des explications quant aux raisons pour lesquelles l'équité d'une procédure d'embauche dépend du contexte et pourquoi il est compliqué de garantir l'équité des traitements automatisés mis en place sur le lieu de travail, voir AlgorithmWatch, pp. 34 ss.

404 EPINEY, § 9, N 27.

405 En droit européen, cet aspect du principe de proportionnalité est explicitement consacré à l'art. 5 let. c (minimisation des données) et e (limitation de la conservation) RGPD ; en droit du Conseil de l'Europe, le principe de proportionnalité est consacré à l'art. 4 al. 1er et 4 let. c de la Convention 108+.

406 MORGENROTH, p. 113.

407 PFPDT, 28e Rapport d'activités, p. 47.

aussi instructif de prendre contact avec l'ancien employeur afin de clarifier quelques questions restées sans réponse lors de l'entretien d'embauche. Le critère de la nécessité s'appréciera toutefois toujours au cas par cas à la lumière des données personnelles traitées et de l'emploi mis au concours[408].

Dans un troisième et dernier temps, l'employeur doit se demander si le fait de soumettre un candidat à un profilage est raisonnable au sens de l'art. 6 al. 2 LPD (proportionnalité au sens strict). La réponse à cette question impose toujours une pesée des intérêts qui varie d'un cas à un autre[409]. On rappellera que lors de cette pesée des intérêts, il faudra tenir compte du droit constitutionnel à l'autodétermination en matière informationnelle de la personne concernée[410] et que cette pesée des intérêts influencera non seulement l'analyse de la proportionnalité du profilage, mais aussi si le consentement ou l'intérêt prépondérant privé éventuellement invoqué par l'employeur en aval doit être considéré valide ou pas[411]. Ainsi, dans le cadre de cette pesée des intérêts, plusieurs aspects pourraient être pris en compte, comme p. ex. :

— le secteur économique concerné ;
— la teneur de l'information préalablement soumise par les candidats ;
— le fondement du profilage (évaluations précédentes de collaborateurs exceptionnels ou, au contraire, évaluations faites par un sous-traitant qui ne connaît que peu, voire pas du tout l'entreprise recrutant un nouveau collaborateur [*data broker*]) ;
— la catégorie des données traitées (données rendues publiques ou données [potentiellement sensibles] acquises auprès de tiers [art. 30 al. 3 LPD]) ;
— l'information soumise au candidat au préalable et/ou après le profilage.

Cela étant, on peut se poser la question plus fondamentale de savoir si « le fait d'opposer mécaniquement les choix et les actions d'autres personnes à un être humain revient à le déposséder de sa propre liberté de choix et d'action » et, dans l'affirmative, considérer que « cela porte atteinte d'une gravité extrême à sa liberté individuelle et à son droit d'autodétermination, dont [on] peut se

408 Dans le même sens, notamment à propos des entreprises de tendance (*Tendenzbetriebe*), voir KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 63 ; pour une position (encore) plus stricte, voir MEIER, Big Data, pp. 60 s.

409 EPINEY, § 9, N 24.

410 EPINEY, idem.

411 À juste titre, HEUBERGER relève que le principe de proportionnalité, notamment sa troisième composante, vient compléter les motifs justificatifs consacrés à l'art. 31 LPD, voir HEUBERGER, N 234 s.

demander si elle ne touche pas au noyau intangible de ces droits »[412]. Si l'analyse proposée par MONTAVON est suivie, les intérêts des candidats devraient toujours primer sur ceux de l'employeur. La liste des intérêts cités ci-dessus serait superflue, le profilage effectué lors d'une procédure d'embauche devrait être qualifié de « déraisonnable » au sens de la LPD.

Dès lors, le profilage dans le cadre d'une procédure d'embauche ne semble pas être conforme au principe de proportionnalité dans la mesure où ce traitement de données n'apparaît pas apte au sens de la LPD. En fonction de l'approche préconisée, le profilage devra également être considéré contraire aux critères de nécessité et de proportionnalité au sens strict.

3. Les principes de finalité et de transparence (art. 6 al. 3 LPD)

Les principes de finalité et de transparence – principes généraux relevant spécifiquement du droit de la protection des données[413] – ont été reformulés dans le cadre de la révision et consacrés à l'art. 6 al. 3 LPD. En effet, afin de rendre l'aLPD plus en ligne avec la lettre de l'art. 5 al. 4 let. b Convention 108+, le Législateur suisse a décidé de reformuler les alinéas 3 et 4 de l'art. 4 aLPD. Cette nouvelle formulation n'implique toutefois aucune modification matérielle[414]. Ainsi, en vertu de cette nouvelle disposition « les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée (principe de transparence) et doivent être traitées ultérieurement de manière compatible avec ces finalités (principe de finalité) ».

En vertu du principe de transparence, et la collecte de données personnelles elle-même et le but de cette collecte doivent être communiqués de manière transparente à la personne concernée. Le principe de transparence est, en principe, présumé respecté lorsque la collecte et le but d'un traitement ont été communiqués à la personne concernée en amont du traitement envisagé, que le traitement est prévu dans une loi ou qu'il découle clairement des circonstances d'espèce[415].

412 À la suite de ces développements, MONTAVON cite l'exemple d'un profilage effectué par la justice pénale nécessairement soumis aux dispositions de droit public. À mon sens, ces développements peuvent également ouvrir une piste de réflexion dans le cadre de l'emploi, voir MONTAVON, p. 664. Le Comité des Ministres s'exprime également sur un ton critique (mais moins tranchant) par rapport au fait d'opposer à un individu des données personnelles qui appartiennent à d'autres personnes, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 53.

413 EPINEY, § 9, N 30.

414 FF 2017 6644.

415 FF 2017 6644.

Le respect du principe de transparence constitue également une précondition de l'exercice du droit d'accès tel que consacré à l'art. 25 LPD[416]. En effet, si la personne concernée n'a pas même connaissance du traitement de données la concernant, il lui sera impossible de faire valoir son droit d'accès[417] et/ou de porter plainte pour atteinte illicite à sa personnalité sur la base de l'art. 32 LPD.

Or, on notera que la consécration d'une obligation de rendre l'algorithme utilisé dans le cadre d'un profilage sur le lieu de travail complètement transparent ne semble pas être une « solution miracle ». En effet, une transparence accrue peut conduire à ce que certaines données sensibles relatives au candidat soient révélées. De plus, une transparence plus importante pourrait également avoir pour conséquence que l'algorithme soit déjoué par les candidats[418].

Le but du principe de finalité, quant à lui, fixe, d'une part, que les données doivent être collectées dans un but déterminé en amont de cette collecte. Ainsi, ce principe interdit la collecte de données dans un but vague, notamment dans l'espoir que ces données serviront un jour[419] (*Verbot der Vorratsdatenspeicherung*). D'autre part, ce principe a pour but de garantir que les données personnelles ne soient pas extraites de leur contexte initial et acquièrent, à la suite de leur décontextualisation, une signification qu'elles n'avaient pas lorsqu'elles ont été mises à disposition par la personne concernée[420]. Or, c'est précisément

416 Le droit d'accès est l'un des piliers du droit de la protection des données et contribue à réaliser le droit à la l'autodétermination en matière informationnelle tel que consacré à l'art. 13 al. 2 Cst. ; pour une analyse plus approfondie du droit fondamental à l'autodétermination en matière informationnelle et le droit d'accès, voir EPINEY/FASNACHT, § 11, N 16 avec des références jurisprudentielles supplémentaires ; dans une veine similaire, FÜZESSÉRY et SCHNEIDER rappellent que « ce n'est que si la personne concernée sait que des données la concernant sont traitées qu'elle en a la maîtrise et qu'elle peut donc décider à quelles conditions elles peuvent être traitées (principe de l'autodétermination informationnelle) », voir FÜZESSÉRY/SCHNEIDER, p. 147.

417 En droit européen, ce lien entre le principe de transparence et le droit d'accès est parfois désigné sous le terme de *Magna Carta* des droits des personnes concernées, voir WACHTER/MITTELSTADT/FLORIDI, p. 83.

418 À ce sujet, le rapport d'*AlgorithmWatch* rappelle que la consécration d'« [traduction] une transparence des algorithmes peut donner lieu à des tentatives de manipulation des algorithmes : le fait de connaître les indicateurs de performance (*proxies*) utilisés peut porter atteinte au but poursuivi par l'algorithme, c'est-à-dire qu'il ne s'agit plus de travailler correctement [pour les employés évalués] mais de maximiser l'unité de mesure utilisée comme indicateur de performance» », voir AlgorithmWatch, p. 32.

419 MEIER, Big Data, p. 61 ; HEUBERGER, N 237.

420 Pour un exemple, on pensera à la comparaison entre une « procédure d'embauche traditionnelle » et une procédure d'embauche fondée sur une évaluation automatisée – développée plus haut dans le cadre de l'analyse du principe de proportionnalité – qui risque de ne pas prendre en compte le contexte, qui peut pourtant être déterminant afin de bien comprendre le parcours d'une personne candidate ; pour une explication plus abstraite des dangers d'une telle décontextualisation, voir ROUVROY, pp. 10 ss.

la vocation des *data brokers* que de générer de nouvelles connaissances sur la base de données (anciennes) déjà disponibles[421].

Il va sans dire que dans l'hypothèse dans laquelle l'employeur a recours aux services d'un sous-traitant qui a acquis des données relatives à un candidat dans le but de les évaluer grâce à un processus automatisé, ce sous-traitant aura vraisemblablement procédé à ce traitement de données en modifiant la finalité du traitement initial (violation du principe de finalité) à l'insu du candidat (violation du principe de transparence). En effet, il est difficilement imaginable qu'une personne ait la prémonition (et de surcroît y consente) à ce que ses habitudes d'achats, ses conversations sur *Tinder* et ses déplacements privés soient évalués afin de déterminer s'il convient de lui offrir un certain emploi ou pas. Ainsi, ces deux principes, regroupés au sein d'une seule disposition de la nLPD, semblent être systématiquement violés lorsqu'un employeur a recours au profilage dans le cadre d'une procédure d'embauche[422].

4. Le principe d'exactitude (art. 6 al. 5 LPD)

Tout comme les principes de finalité et de transparence, le principe d'exactitude est un principe général relevant spécifiquement du droit de la protection des données. Les contours de ce principe ont été précisés lors de la révision totale de l'aLPD[423]. Ainsi, l'art. 6 al. 5 LPD fixe que « celui qui traite des données personnelles doit s'assurer qu'elles sont exactes ». À cette fin, « il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié de la mesure dépend notamment

421 À juste titre, ROUVROY rappelle qu'il convient de distinguer les traitements de données effectués à des fins de recherche (protégés par le privilège de la recherche) et ceux effectués dans un seul but commercial, qui peuvent poser des risques pour les droits des individus concernés, voir ROUVROY, pp. 25 s.

422 Dans le même sens, avec de plus amples développements et un accent tout particulier sur le lien entre ces deux principes et la validité du consentement éventuellement nécessaire afin de justifier le traitement de données envisagé, voir HEUBERGER, N 239 ss. ; dans le même sens à propos du *data mining* (processus par lequel certaines données sont combinées entre elles afin de générer une nouvelle source de connaissance) et du *data warehousing* (processus qui permet de collecter des données sur une longue durée afin de les traiter en fonction des besoins des utilisateurs et de les mettre à disposition ultérieurement), qui constituent les deux premières étapes du profilage, voir EPINEY, § 9, N 34 ; pour un résumé des travaux du Groupe « Article 29 » Protection des données quant aux possibilités de réinterpréter ces principes à la lumière des développements des nouveaux traitements de données, voir MEIER, Big Data, pp. 62 s. À juste titre, MEIER rejette ces propositions ; pour un rejet allant dans le même sens, voir HEUBERGER, N 238.

423 FF 2017 6646 ; pour une comparaison avec les explications très brèves quant à la portée du principe d'exactitude figurant dans le Message relatif à l'aLPD, voir FF 1988 II 457 s.

du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées ».

Lors d'un profilage effectué dans le cadre d'une procédure d'embauche, plusieurs sources d'erreur potentielles peuvent conduire à une évaluation inexacte[424]. Ainsi, à titre d'exemple, il peut arriver que le *data broker* mandaté évalue certains aspects personnels du candidat sur la base de données erronées, p. ex. parce que les données évaluées appartiennent à une personne du même nom[425] ou que les données évaluées ne reflètent plus la situation actuelle de la personne concernée[426]. En outre, la corrélation établie dans le cadre du *data mining* (deuxième étape du profilage) peut s'avérer inexacte (et non une des données évaluées par l'algorithme)[427].

Comme nous l'avons vu plus haut déjà, le raisonnement qui sous-tend une telle évaluation automatisée est souvent incompréhensible. Respecter ce principe s'avère alors compliqué dans la mesure où la rectification d'une évaluation inexacte implique, en amont, de comprendre le raisonnement qui soustend l'évaluation contestée. En d'autres termes, il n'est pas possible de rectifier une corrélation établie automatiquement[428].

De plus, dans une veine plus abstraite, il convient de noter qu'il peut s'avérer difficile pour l'employeur de vérifier l'exactitude des données évaluées par son sous-traitant. Malgré cette difficulté pratique, l'employeur reste responsable du traitement au sens de l'art. 5 let. j LPD. Cet état de fait est d'autant plus regrettable que le profilage porte sur les données personnelles d'une personne encore inconnue et que cette dernière n'a très souvent pas connaissance de ce traite-

424 Voir *supra* Chapitre 5. Avantages et risques.

425 Pour un exemple qui reste d'actualité, voir FF 1988 II 457 qui se lit comme suit : « Une caisse de recouvrement, qui aurait confondu deux personnes portant le même nom et habitant dans la même rue, peut être amenée à engager à tort des poursuites contre une personne qui n'est pas son débiteur » ; pour un exemple similaire, mais plus récent et impliquant une évaluation automatisée, voir MORGENROTH, pp. 31 ss.

426 On pensera, à titre d'exemple, à une évaluation automatisée de données personnelles toujours disponibles sur Internet (ou dans une quelconque autre base de données) bien après que les événements dans le cadre desquels ces données personnelles ont été collectées aient eu lieu. Ces hypothèses renvoient à la question plus générale du « droit à l'oubli ». À ce titre, EPINEY précise, à juste titre, que « [traduction] le principe d'exactitude est violé lorsque le responsable du traitement traite des données manifestement inexactes, indépendamment du fait que ces données inexactes influencent ou non l'évaluation globale (*Gesamtbild*) envisagée », voir EPINEY, § 9, N 47.

427 L'exemple le plus connu est sans doute celui de la procédure de recrutement automatisée mise en place au sein de l'entreprise américaine *Amazon* en 2014 puis abrogée trois ans plus tard dans la mesure où elle s'est avérée discriminatoire envers les femmes, voir *supra* Chapitre 5. Avantages et risques ; pour des précisions quant aux raisons pour lesquelles le calcul de corrélations peut être une source d'erreurs, voir ROUVROY, pp. 10 ss.

428 Dans le même sens, voir MEIER, Big Data, p. 66.

ment de données. En d'autres termes, l'employeur ne pourra pas vérifier si l'évaluation faite par le sous-traitant correspond (plus ou moins) à sa propre évaluation. Ignorant qu'un profilage a été effectué, le candidat n'aura pas la possibilité de corriger, voire de justifier une évaluation qui serait inexacte, voire erronée selon lui.

Il découle de ce qui précède, qu'il peut s'avérer difficile, voire impossible pour l'employeur responsable du traitement de garantir la bonne application du principe d'exactitude des données, notamment lorsqu'il souhaiterait trouver la source d'erreur dans le cadre d'une contestation d'une évaluation effectuée par un *data broker*. Ceci est d'autant plus vrai dans la mesure où le Tribunal administratif fédéral ne semble pas imposer de très hauts standards quant aux obligations incombant aux responsables de bases de données exploitées[429].

5. Le principe de sécurité des données (art. 8 LPD)

Le principe de sécurité des données nouvellement consacré à l'art. 8 LPD exige du responsable du traitement et des sous-traitants éventuels qu'ils assurent, « par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru ». Les contours de cette obligation qui pèse sur le responsable du traitement ont été fixés par voie d'ordonnance[430].

La difficulté quant à la bonne application de cette disposition tient au fait que ni la LPD ni le PFPDT ni le Tribunal administratif fédéral ne précisent ce qui doit être entendu par « mesures appropriées »[431] et que cette évaluation s'effectuera toujours au regard de l'état de la technologie au moment du litige[432].

429 Ainsi, à propos de l'arrêt du Tribunal administratif fédéral du 18 avril 2017 (A-4232/2015) *Moneyhouse*, MÉTILLE et XUAN précisent que « tant le PFPDT que le TAF admettent premièrement qu'il suffit de contrôler la véracité des données communiquées (un maître de fichier [notion connue sous le régime de l'aLPD désignant le responsable du traitement de données] peut donc conserver des données potentiellement fausses s'il ne les exploite pas activement) et deuxièmement les contrôles ne doivent pas porter sur l'ensemble des données communiquées, mais seulement sur un pourcentage relativement faible ». Dans ce contexte, on rappellera que s'il est vrai que cet arrêt a été rendu sous le régime de l'aLPD, qui ne consacrait pas de définition du profilage, le traitement litigieux aurait pu être qualifié de profilage, voir MÉTILLE/XUAN, p. 179.

430 Art. 1 à 5 OPDo.

431 Dans le cadre de leur analyse de l'arrêt du Tribunal administratif fédéral du 18 avril 2017 (A-4232/2015) *Moneyhouse*, MÉTILLE et XUAN déplorent ce manque de précision quant aux contours exacts du principe de sécurité, voir MÉTILLE/XUAN, p. 179. La révision de l'aOLPD a apporté quelques précisions quant aux contours de ce principe.

432 L'art. 8 al. 3 aOLPD qui fixait que « ces mesures [techniques et organisationnelles] font l'objet d'un réexamen périodique » a été repris à l'art. 1er al. 5 OPDo qui prévoit désormais que « le besoin de protection des données personnelles, le risque encouru, ainsi que les mesures techniques et organisationnelles sont réévalués pendant toute la durée du traitement ».

Ainsi, étant donné que les moyens techniques évoluent très rapidement[433] et parfois de façon inattendue pour les non-spécialistes, il peut s'avérer difficile, pour le responsable du traitement, de respecter cette obligation légale. En effet, comme dans le cadre de l'analyse du respect des principes généraux consacrés à l'art. 6 LPD, chercher à savoir si un employeur a respecté le principe de sécurité des données s'appréciera au cas par cas et toujours à la lumière des développements techniques récents. Cet état de fait implique une insécurité juridique pour le recruteur qui devra, au fil du temps qui passe, se demander s'il a pris toutes les mesures exigibles au moment de chaque procédure d'embauche. À ce titre, il convient de soulever quelques problèmes supplémentaires de mise en œuvre.

D'abord, en tant que responsable du traitement, l'employeur qui procède au profilage reste responsable pour la sécurité des données[434]. Or, l'employeur n'a ni le contrôle (physique) sur la collecte des données ni sur leur évaluation automatisée. Ainsi, si l'employeur veut honorer ses obligations légales, il lui incombe de s'assurer, par voie contractuelle, que le *data broker* auquel il fait appel garantisse la sécurité des données. À la difficulté de déterminer ce qui constituent des « mesures appropriées » s'ajoute un défaut de sensibilisation à la thématique qui peut entraîner de lourdes conséquences pour l'image de l'employeur. En effet, en raison de ce défaut de sensibilisation, nombreux sont les employeurs qui ne respectent pas cette obligation en amont – au risque de subir une plainte (peu probable) ou une atteinte à leur réputation en tant qu'employeur (plus probable à moyen terme et plus grave)[435].

Ensuite, il convient de clarifier la distinction entre les obligations qui découlent de l'art. 7 LPD qui fixe le cadre de la protection des données dès la conception (*privacy by design*) et par défaut (*privacy by default*) et celles qui découlent de l'art. 8 LPD. La protection des données dès la conception d'une part et par défaut d'autre part imposent, au même titre que l'art. 8 LPD, la mise en place de mesures techniques et organisationnelles qui « doivent être appropriées au regard notamment de l'état de la technique, du type de traitement et de son étendue, ainsi que du risque que le traitement des données présente pour la personnalité ou les droits fondamentaux des personnes concernées ». Il découle de ces quelques constatations que les champs d'application de ces deux dispositions risquent de se recouper en pratique. Bien distinguer le champ

433 À titre d'exemple, on pensera aux possibilités de plus en plus répandues de procéder à la ré-identification de données anonymes, voir ROUVROY, pp. 20 ss.

434 Art. 5 let. j LPD et art. 8 al. 1er LPD.

435 Dans le même sens à propos de la *Deutsche Bahn* et d'autres employeurs allemands dont la réputation a été très affectée à la suite de la révélation de mesures de surveillance secrète mises en place à l'encontre de leurs employés, voir WIELE, pp. 685 ss.

d'application de ces deux dispositions est toutefois important dans la mesure où la violation de l'art. 8 LPD constitue une violation de la personnalité qui peut éventuellement être justifiée par un motif justificatif. La violation de l'art. 7 LPD ne constitue pas une violation du droit de la personnalité au sens de la LPD, mais peut engendrer des conséquences relevant du droit de la responsabilité[436].

Enfin, l'articulation entre l'art. 8 LPD et la définition de « violation de la sécurité des données » telle que prévue à l'art. 5 let. h LPD devra être clarifiée par les tribunaux. En effet, on rappellera que l'art.5 let. h LPD fixe qu'« on entend par : *violation de la sécurité des données* (sic): toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données ». Si la notion de « violation de la sécurité des données » est reprise à l'art. 8 al. 2 LPD, l'al. 1er mentionne la notion de « sécurité adéquate » et l'al. 3 mentionne le concept d'« exigences minimales en matière de sécurité des données ». Si le Message n'apporte aucune précision quant à l'articulation de ces diverses dispositions, il ressort du Rapport explicatif sur la révision de l'OPDo du 31 août 2022 que « toute violation de la sécurité des données au sens de l'art. 5 let. h LPD ne constitue pas une violation des exigences minimales au sens de l'art. 8 al. 3 LPD et donc une violation des devoirs de diligence au sens de l'art. 61 let. c LPD. On ne peut ni ne doit exiger une sécurité absolue. Il est en effet concevable que le responsable du traitement ait pris toutes les mesures adéquates, mais que la sécurité des données soit malgré tout violée en raison du risque résiduel : cela ne saurait être imputé au responsable. Dans le cadre des exigences minimales, il importe surtout de vérifier si le responsable du traitement et le sous-traitent ont pris des mesures adéquates dans le cas concret, qu'il y ait eu une violation de la sécurité des données ou non »[437]. En d'autres termes, l'articulation entre les art. 5 et 8 LPD devra faire l'objet de clarifications jurisprudentielles.

Il découle de cette brève analyse que les contours du principe de sécurité des données sont vagues, constituant une insécurité juridique supplémentaire à prendre en considération par l'employeur qui souhaiterait soumettre un candidat à un profilage. Cela étant, ROUVROY précise, à juste titre, que les violations du principe de sécurité n'engendrent pas les plus grands risques pour les droits

436 ROSENTHAL, Das neue Datenschutzgesetz, N 43 ; position reprise par KAUFMANN/SCHUERCH, Digitalisierung und Privatsphäre im Arbeitsverhältnis, p. 47. On rappellera toutefois, qu'en principe, la liste des cas de violations de la personnalité consacrée à l'art. 30 LPD n'est pas exhaustive, voir FF 2017 6688. En d'autres termes, un tribunal saisi pourrait éventuellement aboutir à la conclusion que la violation de l'art. 7 LPD constitue également une violation de la personnalité.

437 OFJ, Rapport explicatif sur la révision de l'ordonnance sur la protection des données, p. 21.

des personnes concernées. Elle estime que l'utilisation bien intentionnée, mais peu réfléchie des nouvelles formes de traitements de données constitue un risque bien plus important pour lesdits droits[438].

6. L'interdiction de transferts de données sensibles à des tiers (art. 30 al. 2 let. c LPD)

À titre préliminaire on notera que l'interdiction de transférer des données sensibles à des tiers telle que fixée à l'art. 30 al. 2 let. c LPD ne découle pas directement du droit de la personnalité tel que consacré à l'art. 28 du Code civil et dont la LPD se fait l'écho. Cette nouvelle disposition avait été introduite dans l'aLPD en raison d'une disposition similaire en droit européen[439].

De manière assez surprenante, cette disposition semble prévoir des exigences moins strictes que l'ancien droit dans la mesure où la notion spécifiquement suisse du profil de la personnalité a été éliminée dans le cadre de la révision de l'aLPD[440]. En effet, l'aLPD interdisait, en principe, le transfert de données sensibles *et de profils de la personnalité* à des tiers[441].

Si cette modification du régime légal est regrettable, il convient de noter que cette troisième hypothèse d'atteinte à la personnalité prévue par la LPD ne semble pas jouer un rôle important dans le cadre d'une procédure d'embauche. En effet, cette disposition ne trouvera application uniquement dans l'hypothèse où l'employeur – responsable du traitement – enverrait des données sensibles relatives au candidat à un tiers. Toutefois, il est peu probable qu'au stade de la procédure d'embauche l'employeur dispose de données sensibles à propos du candidat et qu'il les communique à un tiers (dans quel but ?). De surcroît, on notera que dans le cadre de cette contribution, le *data broker* est qualifié de sous-traitant au sens de l'art. 5 let. k LPD et non de tiers au sens de l'art. 30 al. 2 let. b LPD. Cette qualification n'a non seulement un impact sur les motifs justificatifs qui peuvent potentiellement être invoqués, mais aussi sur l'applicabilité de l'art. 30 al. 2 let. c LPD. En d'autres termes, les développements susmentionnés n'auraient qu'une portée dans le cadre de cette contribution si le *data broker* était qualifié de tiers au sens de la LPD[442].

438 ROUVROY, p. 30.

439 Art. 9 al. 1er RGPD.

440 On relèvera toutefois que la notion a été « réintroduite par la petite porte par le biais du profilage à risque élevé », voir, à juste titre, ROSENTHAL, Das neue Datenschutzgesetz, N 27.

441 Art. 12 al. 2 let. c aLPD, italique ajouté par mes soins ; en guise de rappel, l'art. 3 let. d aLPD définissait le profil de la personnalité comme suit : « On entend par : *profil de la personnalité* (sic), un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ».

442 La sous-traitance est régie par l'art. 9 LPD.

7. L'interdiction de traitements contraires à la volonté expresse de la personne concernée (art. 30 al. 2 let. b LPD)

En vertu de l'art. 30 al. 2 let. b LPD « constitue notamment une atteinte à la personnalité le fait de traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée ».

L'interdiction de traitements contraires à la volonté de la personne concernée que ROSENTHAL désigne sous le nom de « principe général du *opt-out* » consacrée à l'art. 30 al. 2 let. b LPD est un principe clef en droit de la protection des données suisse dans la mesure où – contrairement au droit européen – le droit suisse ne prévoit pas l'obligation que tout traitement de données doit se fonder sur un motif justificatif. Ainsi, un traitement de données est illicite uniquement s'il est contraire aux principes généraux *et* qu'il ne peut pas être justifié *ou* si la personne s'y est opposé de manière expresse. Pour ce faire, elle ne doit pas avancer une raison particulière. Cette approche est particulièrement libérale et reflète une interprétation du droit fondamental à l'auto-détermination en matière informationnelle ancrée dans la responsabilité individuelle.

Il découle de cette constatation que si une personne privée, p. ex. l'employeur ou un *data broker*, procède à un traitement de données et respecte les principes généraux, elle peut y procéder tant que la personne concernée ne s'y est pas expressément opposé. En d'autres termes, le consentement exprès de la personne concernée, p. ex. du candidat, n'est pas nécessaire afin d'effectuer le traitement de données envisagé. Il convient de noter que ROSENTHAL explique que cette analyse est valable également lorsque le traitement de données initial est un profilage[443]. Selon cet auteur, tant que le profilage est proportionné au sens de l'art. 6 al. 2 LPD, il pourra être effectué sans que la personne doive y consentir.

Ce principe supporte toutefois une exception. L'art. 5 al. 7 LPD fixe que lorsqu'un traitement porte sur des données sensibles ou constitue un profilage à risque élevé, la personne concernée doit expressément y consentir. En d'autres termes, le principe du *opt-out* ne semble pas être applicable dans ces hypothèses et soulève une nouvelle fois l'interrogation de ce qui doit être entendu par profilage et par profilage à risque élevé respectivement. Comme nous l'avons vu plus haut, un profilage effectué pendant une procédure d'embauche peut être qualifié de profilage à risque élevé qui conduit potentiellement à un

443 ROSENTHAL semble toutefois reconnaître qu'il en va autrement s'il s'agit d'un « profilage à risque élevé », voir ROSENTHAL, Das neue Datenschutzgesetz, N 38b.

traitement de données sensibles (p. ex. à la suite de calculs de corrélations inattendues). Un employeur ne saurait donc légitimer le profilage en faisant valoir que le candidat ne s'y est pas expressément opposé.

Dans le cadre d'une procédure de recrutement, le profilage semble dès lors être contraire au :

— principe de proportionnalité (en raison de l'incertitude liée à la question de savoir si un tel traitement de données est apte à recruter le meilleur candidat pour un emploi donné et s'il est raisonnable d'opposer le comportement d'une personne tierce au candidat qui, pour des raisons qu'il ignore, se trouve partager certaines caractéristiques avec ce tiers inconnu) ;
— principe de finalité (en raison d'une collecte de données à des fins imprévisibles pour la personne concernée au moment de cette collecte).

Une violation des autres principes généraux est également concevable, même si de telles violations sont moins évidentes. Il en va ainsi du principe de transparence si la personne concernée n'a pas été informée par rapport au profilage effectué. Il en va de même du principe d'exactitude lorsque les données traitées sont inexactes car fausses ou trop anciennes et/ou que les calculs effectués aboutissent à une évaluation erronée, p. ex. à la suite d'une erreur de programmation. Si le profilage a été effectué à l'insu du candidat, le traitement aura porté atteinte au principe de la bonne foi. Si le profilage est qualifié de profilage à risque élevé et que le candidat n'y a pas expressément consenti, le traitement de données aura été effectué en violation de l'art. 30 al. 2 let. b LPD.

Il découle des développements ci-dessus que lorsqu'un profilage est effectué dans le cadre d'une procédure d'embauche, ce nouveau traitement de données peut potentiellement porter atteinte à plusieurs principes généraux ou être contraire à l'art. 30 al. 2 let. b LPD. Toutefois, si l'employeur peut faire valoir un des motifs justificatifs fixés à l'art. 31 LPD, il peut alors rendre le traitement licite. Tout comme l'art. 13 al. 1er aLPD, l'art. 31 LPD prévoit quatre motifs justificatifs[444] dont il convient de déterminer l'applicabilité dans le contexte d'un profilage effectué lors d'une procédure d'embauche.

444 FÜZESSÉRY et SCHNEIDER précisent à ce sujet que les craintes selon lesquelles les entreprises ne pourraient dorénavant uniquement procéder à un profilage sur la base du consentement des personnes concernées sont infondées dans la mesure « où d'autres motifs peuvent entrer en ligne de compte pour justifier un profilage, tels que l'existence d'un intérêt privé ou public prépondérant », voir FÜZESSÉRY/SCHNEIDER, p. 145 ; dans le même sens, voir HEUBERGER, N 214 ; en droit européen, six motifs justificatifs sont prévus, voir art. 6 RGPD et, pour plus de précisions à ce sujet, Agence des droits fondamentaux de l'UE et Conseil de l'Europe, p. 126.

D. Les motifs justificatifs (art. 31 LPD)

En vertu de l'art. 31 al. 1er LPD, le consentement de la personne concernée (1), un intérêt privé prépondérant (2), un intérêt public prépondérant (3) ou une loi prévoyant le traitement (4) peut justifier un traitement de données en principe illicite. À ce stade, il convient de noter que si l'employeur est considéré comme responsable du traitement et que le *data broker* est son sous-traitant au sens de l'art. 5 let. k LPD, l'employeur et son sous-traitant peuvent faire valoir les mêmes motifs justificatifs[445]. On rappellera également que savoir si un des motifs justificatifs peut être invoqué pour justifier un traitement de données effectué dans le cadre d'une procédure d'embauche est controversée allant au-delà du cadre fixé par l'art. 328b CO et n'a pas (encore) été tranchée de manière définitive par le Tribunal fédéral[446]. Dans le but de proposer une analyse aussi complète que possible de la thématique définie, savoir si l'un des motifs justificatifs peut en effet être invoqué est soulevé même si cette question pourrait se révéler superflue en fonction de la jurisprudence future.

1. Le consentement du candidat

À titre préliminaire, on rappellera qu'en vertu du principe du *opt-out* (*Grundsatz der « Erlaubnis mit Verbotsvorbehalt »*) le consentement a une portée moins importante en droit suisse qu'en droit européen[447] de la protection des données.

Si un traitement de données envisagé viole un des principes généraux, l'art. 31 al. 1er LPD mentionne, comme premier motif justificatif, le consentement de la personne concernée et consacre ainsi un aspect central du droit à l'autodétermination en matière informationnelle de la personne concernée[448]. L'art. 6 al. 6 LPD quant à lui vient définir le consentement au sens de la LPD. Ainsi, en vertu de cette disposition « la personne concernée [...] ne consent valablement que si elle exprime librement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée »[449]. Un consentement valide se caractérise donc par les trois éléments cumulatifs suivants :

445 Art. 9 al. 4 LPD.

446 Pour un résumé des deux positions défendues en doctrine et de multiples références supplémentaires, voir KASPER/WILDHABER, pp. 196 ss.

447 Art. 6 al. 1er RGPD ; pour plus de précisons quant à la portée du consentement en droit européen, voir SPIECKER GENANNT DÖHMANN, p. 347.

448 MEIER, Protection des données, N 824.

449 Le consentement en droit de la protection des données est qualifié, par une majorité de la doctrine, comme acte juridique unilatéral. Ainsi, les dispositions pertinentes figurant dans le CC et le CO seraient applicables par analogie en droit de la protection des données, pour une analyse plus approfondie de cette qualification et de ses implications en pratique, voir FASNACHT, N 220 ss.

— un consentement libre ;
— un consentement limité à un ou plusieurs traitements déterminés en amont ;
— un consentement donné après une information en bonne et due forme.

La définition légale du « consentement » n'a pas été modifiée dans le cadre de la révision de la LPD[450]. Ce qui a pu être écrit quant au consentement sous le régime de l'aLPD reste donc valable. Ainsi, quelques spécificités du consentement en droit de la protection des données, qui existaient déjà sous l'aLPD, méritent d'être analysées.

a. Les conditions de fond

D'abord, ce qui doit être entendu par « consentement libre » n'est que peu clair. En vertu de la jurisprudence du Tribunal fédéral, des matériaux et de la doctrine majoritaire, un consentement n'est *pas* libre au sens de la LPD lorsqu'en cas de refus, la personne concernée risque de subir des désavantages *ou* que le consentement est dépourvu de lien direct avec la finalité du traitement de données *ou* qu'il semble être disproportionné pour d'autres raisons[451]. Pour d'autres encore, le consentement ne saurait être considéré libre si la personne concernée ne dispose pas de réelles alternatives[452]. Tel serait le cas si le responsable du traitement a une position dominante ou si la relation entre le responsable du traitement et la personne concernée est caractérisée par une dépendance sociale ou factuelle importante[453].

Une partie de la doctrine considère que le recruteur et le candidat négocient sur un pied d'égalité et que le lien de subordination qui caractérise les relations entre employeur et employé ne se met en place qu'une fois la relation de travail entamée. À la lumière de ces développements, le consentement du candidat semble pouvoir être donné librement faute d'un quelconque lien de dépendance[454]. Or, comme nous l'avons vu plus haut déjà, la procédure de

450 La définition du consentement n'a été que légèrement remaniée afin de permettre un rapprochement entre la définition suisse et la terminologie proposée par la Convention 108+, voir FF 2017 6647.

451 FF 2017 6647 s. ; dans le même sens, voir EPINEY, § 9, N 18.

452 EPINEY, § 9, N 18.

453 Sur ce point, les conditions d'un consentement libre rejoignent celles d'un consentement libre en droit général de la personnalité selon lesquelles le consentement ne saurait être considéré libre si la liberté est considérablement réduite en raison d'une quelconque dépendance, voir VASELLA, Einwilligung, N 17 s.

454 Voir *supra* Chapitre 7. Le Code des obligations.

recrutement est souvent ressentie comme une première phase de la relation de subordination. Le candidat voudra satisfaire les attentes de son futur employeur non seulement pendant la relation de travail, mais aussi (et surtout) pendant la procédure d'embauche. Ainsi, une autre partie de la doctrine considère que le lien de subordination se met en place (du moins partiellement) pendant la procédure d'embauche[455]. Ce lien aurait alors pour conséquence que les parties ne négocient pas sur un pied d'égalité et que le candidat concerné ne peut pas librement donner son consentement à un quelconque traitement de données. Dès lors, en fonction de la position retenue, le consentement d'un candidat à se soumettre à un profilage sera qualifié de libre ou pas. En pratique, se demander si le consentement d'un candidat est libre ou pas s'appréciera très vraisemblablement avec une certaine retenue au cas par cas, notamment en prenant en compte les pratiques du secteur concerné et les opportunités de la personne concernée sur le marché du travail.

Dans une veine plus générale, on rappellera que la plupart du temps, les individus consentent de manière (presque) automatisée à la collecte de leurs données personnelles[456] (qui seront, le cas échéant réutilisées dans le cadre d'une procédure d'embauche). ROUVROY avance plusieurs raisons possibles à un tel consentement (presque) automatisé : les personnes concernées estiment « n'avoir rien à cacher », la commodité d'un service disponible immédiatement après avoir consenti à la collecte desdites données ou encore les avantages perçus d'interagir avec d'autres individus. Cela est d'autant plus vrai qu'effacer ses empreintes numériques suppose la mise en place de mesures parfois complexes parce que la plupart des services dont l'accès implique une collecte de données fonctionnent selon le principe du *opt-out*[457]. Face aux nombreux services qui fonctionnent sur la base d'une collecte importante de données personnelles, on peut dès lors se poser la question plus générale de savoir si le consentement donné par le candidat afin d'accéder à l'un de ces services (ou, le cas échéant, à un emploi) a été donné librement au sens de la LPD. À la lumière de ces développements, il est regrettable que le Législateur suisse ne se soit pas inspiré du droit européen. En effet, contrairement à ce qui a pu être expressément prévu en droit de l'UE[458], la LPD révisée ne prévoit pas d'interdiction de couplage[459]. Ainsi, en droit suisse, il est en principe possible de faire dépendre

455 Voir *supra* Chapitre 7. Le Code des obligations.

456 Voir *supra* Chapitre 1. D'une surveillance publique à une surveillance privée.

457 Pour de plus amples explications qui relèvent de l'économie comportementale et qui permettent de mieux cerner cette « léthargie », voir ROUVROY, pp. 23 s.

458 Art. 7 al. 4 RGPD.

459 La LPD et le Message du Conseil fédéral restent muets à ce sujet.

la conclusion d’un contrat du consentement de la personne concernée bien qu’une telle constellation puisse avoir pour conséquence de remettre en cause la nature libre du consentement[460].

Ensuite, le consentement doit être donné par rapport à un traitement de données déterminé en amont. À la lumière de cette deuxième condition on peut se demander à quel point le traitement de données doit en effet être déterminé en amont. Devrait-il suffire que l’employeur indique au candidat qu’un profilage sera effectué dans le cadre de la procédure d’embauche ou devrait-il, au contraire, expliquer quelles données personnelles du candidat seront traitées et sous quelle forme ? La question qui se pose ensuite et qui fait écho aux développements relatifs aux principes de finalité et de transparence est celle de savoir comment expliquer un raisonnement incompréhensible même pour ceux qui ont développé l’évaluation automatisée. Ainsi, il semblerait qu’au vu du mode de fonctionnement du profilage, cette deuxième condition ne saurait que très difficilement être respectée. Si toutefois une interprétation généreuse de cette deuxième condition est retenue, l’employeur devra à tout le moins être en mesure d’énumérer les différentes catégories de données personnelles qui seront évaluées afin de permettre au candidat de vérifier si elles sont exactes et, le cas échéant, de s’opposer au traitement de données erronées (art. 32 al. 1er LPD) et/ou dépourvues de lien avec l’emploi envisagé (art. 32 al. 2 let. a LPD).

En outre, un consentement n’est valable qu’après une information mise à disposition en bonne et due forme. S’il semble évident qu’un consentement ne peut qu’être considéré libre s’il est donné après une information complète (qui ne doit pourtant pas englober une mention spécifique quant au droit de la personne concernée à retirer son consentement en tout temps), il n’est que peu clair à quelles autres exigences une information valable doit pouvoir répondre. Face aux nouveaux traitements de données personnelles on peut se demander avant tout à quel moment cette information doit intervenir[461].

Par ailleurs, sur une note plus concrète, cette disposition n’exclut pas qu’un mineur puisse valablement consentir à un traitement de données. Sur ce point également, le droit suisse est moins strict que le droit de l’UE[462] et les recommandations du Conseil de l’Europe[463]. Cette possibilité laissée par le droit

460 Art. 7 al. 3 LPD ; pour les limites à cette possibilité laissée au responsable du traitement, voir ROSENTHAL, Das neue Datenschutzgesetz, N 30 et 51 ; pour une interprétation très généreuse du défaut d’une telle interdiction en droit suisse, voir BÜHLMANN/SCHÜEPP, N 29.

461 MEIER, Big Data, pp. 71 s.

462 Art. 8 RGPD ; pour plus de détails quant à la portée de cette disposition, voir Groupe de travail « Article 29 », Lignes directrices sur le consentement, pt. 7.1.

463 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l’enfant dans l’environnement numérique, Annexe à la Recommandation CM/Rec (2018)7, pt. 29 s.

suisse pourrait se révéler déterminante p. ex. lorsqu'il s'agit d'examiner la licéité d'un profilage d'un futur apprenti (mineur dans la plupart des hypothèses). Au vu des risques d'atteintes aux droits des personnes concernées peu prévisibles, encore moins pour un mineur, il est particulièrement regrettable que le Législateur ne se soit pas inspiré du droit européen sur ce point afin de prévoir un régime renforcé pour les moins de 18 ans. Cette constatation est d'autant plus vraie à la lumière du devoir d'assistance renforcé qui incombe à tout employeur qui engage un apprenti[464].

Enfin, on retiendra que savoir si un consentement est valable ou non n'entraînera pas de pesée d'intérêts[465]. L'appréciation de ce motif justificatif se distingue alors fondamentalement de l'intérêt prépondérant privé ou public. Toutefois, il n'en demeure pas moins que plus le risque d'une atteinte à la personnalité est important, plus les exigences quant à la validité du consentement sont hautes[466].

Les conditions matérielles du consentement d'un candidat soumis au profilage ainsi esquissées, il convient de se pencher sur les éventuelles conditions de forme d'un tel consentement.

b. Les conditions de forme

En principe, le consentement ne doit répondre à aucune condition de forme. Il peut donc être implicite[467]. Ce principe n'est toutefois pas absolu. En vertu de l'art. 6 al. 7 LPD, qui reprend, en grande partie les exigences fixées à l'art. 4 al. 5 aLPD, le consentement doit être exprès[468] dans trois cas de figure, notamment lorsque qu'il s'agit :

- d'un traitement de données sensibles ;
- d'un profilage à risque élevé effectué par une personne privée ;
- d'un profilage effectué par un organe fédéral[469].

---

464 Pour des explications plus détaillées allant dans ce sens, voir HUGENTOBLER, art. 328 CO, N 2 ; PELLASCIO, art. 328 CO, N 3 ; EMMEL, art. 328 CO, N 2.

465 FF 2017 6689.

466 FF 2017 6647 ; ROSENTHAL, Das neue Datenschutzgesetz, N 30.

467 ROSENTHAL, art. 4 LPD, N 75 et 79.

468 Il convient de clarifier que la notion de « consentement exprès » est synonyme de « consentement explicite », pour les raisons convaincantes d'une telle lecture, voir VASELLA, Einwilligung, N 31.

469 Cette disposition a pour conséquence qu'un profilage effectué par un organe fédéral devra être justifié sur la base de deux motifs justificatifs : une base légale (conséquence du principe de légalité) et le consentement exprès de la personne concernée (conséquence du droit à l'autodétermination en matière informationnelle).

L'exigence renforcée par rapport au profilage à risque élevé est nouvelle et reflète le souci du Législateur de veiller à un meilleur encadrement des traitements portant potentiellement plus lourdement atteinte au droit de la personnalité ou aux droits fondamentaux des personnes concernées[470].

Si les appréciations sur ce qui doit être entendu par consentement exprès varient[471], il convient de s'aligner sur les positions d'EPINEY et de VASELLA qui proposent de définir le consentement exprès en droit de la protection des données tel qu'il est défini en droit des obligations. Ainsi, un consentement exprès serait caractérisé par une expression active de la volonté de la personne concernée. Elle peut être exprimée par oral ou par écrit, voire par voie électronique. Une telle interprétation correspond d'ailleurs au droit européen[472].

Partant du principe qu'un profilage dans le cadre d'une procédure d'embauche constitue un profilage à risque élevé ou aboutit à un traitement de données sensibles du candidat et qu'un tel traitement de données viole au moins un des principes généraux de la LPD, l'employeur devra demander le consentement *exprès* du candidat avant d'effectuer le profilage envisagé. Au-delà de la question controversée de savoir si un consentement peut en effet justifier un profilage effectué par un employeur, cet état de fait suscite une insécurité juridique supplémentaire. Pour des raisons de preuve, il sera très probablement conseillé de demander un tel consentement exprès par écrit. Une telle mesure de précaution semble pourtant être contraire à la volonté du Législateur qui ne souhaitait pas alourdir les obligations des responsables de traitement.

Il découle de ce qui précède qu'il est que peu certain que ce premier motif justificatif puisse justifier un recours au profilage pendant une procédure de recrutement. On peut dès lors se demander si un intérêt prépondérant privé de l'employeur pourrait justifier le profilage d'une personne candidate.

2. Un intérêt privé prépondérant

L'art. 31 al. 2 LPD prévoit une liste non-exhaustive d'intérêts prépondérants privés du responsable du traitement qui pourraient justifier un traitement. L'art. 31 al. 2 let. a LPD semble être le seul exemple pertinent dans le cadre de cette contribution. Cette disposition fixe que « les intérêts prépondérants du responsable du traitement entrent notamment en considération dans les

470 On notera que le projet de loi prévoyait que le consentement devait être exprès pour tous les profilages, voir FF 2017 6647. Il s'agit d'une des modifications de dernière minute, qui n'est pas mentionnée dans le Message.

471 VASELLA, Einwilligung, N 22 ss. ; dans son extensive contribution relative à la nouvelle LPD, ROSENTHAL mentionne les nombreuses questions qui subsistent en pratique quant à savoir ce qui doit être entendu par « consentement exprès », voir ROSENTHAL, Das neue Datenschutzgesetz, N 32.

472 VASELLA, Einwilligung, N 31.

cas [où] le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant ». Cet exemple reprend la logique de l'art. 328b CO qui fixe que « l'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi »[473].

Par le passé, certains contrôles de sécurité extensifs ont pu être justifiés par l'intérêt prépondérant de l'employeur à s'assurer de l'intégrité de ses employés. On pensera, p. ex., aux personnes employées dans le secteur bancaire, pénitencier et des technologies de pointe, où le personnel a accès à des installations et des données sensibles[474]. Ainsi, il s'agit de savoir si dans ces contextes, un profilage pourrait se justifier *mutatis mutandis*. Toutefois, un contrôle de sécurité ne saurait être comparé à un profilage de la personne candidate. La quantité et la qualité des données collectées varie considérablement entre un contrôle de sécurité – même extensif – et un profilage. Contrairement au raisonnement qui sous-tend le profilage, le raisonnement qui sous-tend un contrôle de sécurité (licite) est transparent ce qui permet aux personnes concernées de comprendre un éventuel refus d'embauche et de faire recours en cas de besoin. En d'autres termes, les conséquences juridiques pour les candidats concernés peuvent être très différentes. Dès lors, les motifs justifiant un éventuel contrôle de sécurité ne sauraient être appliqués tels quels dans le cadre du profilage.

De surcroît, il a été confirmé il y a plusieurs années déjà que des motifs économiques pouvaient être invoqués comme intérêt prépondérant privé de n'importe quelle personne partie au traitement[475]. Confrontés aux possibilités offertes par le profilage des candidats, les employeurs pourraient faire valoir que de tels traitements de données sont nécessaires dans la mesure où ils permettraient de réduire les coûts des procédures de recrutements (intérêt prépondérant de l'employeur) et d'analyser un plus grand nombre de candidatures dans un même intervalle de temps (intérêt prépondérant de l'employeur *et* des candidats).

Étant donné que « la jurisprudence [...] ne permet d'admettre qu'avec retenue des intérêts privés [...] prépondérants »[476] il n'est que peu clair dans quel sens un tribunal trancherait cette question. Au vu du nombre grandissant

473 Pour une analyse plus approfondie de cette disposition, voir *supra* Chapitre 7. Le Code des obligations.

474 PFPDT, Explications relatives aux contrôles de sécurité (employés du secteur privé), mars 2015.

475 MEIER, Protection des données, N 1622.

476 Arrêt du Tribunal administratif fédéral du 18 avril 2017 (A-4232/2015) *Moneyhouse*, cons. 5.4.2.3 ; par rapport à la Convention 108, ROUVROY semble être d'avis que les intérêts économiques du responsable du traitement ne sauraient justifier une atteinte à l'autodétermination des personnes concernées, voir ROUVROY, pp. 25 s.

d'employeurs ayant recours au profilage, il se peut qu'un tribunal adopte une position généreuse. En tout état de cause, lorsqu'un traitement est justifié sur la base de l'art. 31 al. 2 let. a LPD, le traitement doit être en lien direct avec la conclusion du contrat. Ainsi, il est difficile d'admettre que l'évaluation des conversations *Tinder* du candidat serait justifiée à la lumière de cette disposition.

Le motif justificatif de l'intérêt prépondérant privé étant le plus controversé en pratique[477], on peut se demander si un intérêt public prépondérant pourrait justifier l'utilisation du profilage.

3. Un intérêt public prépondérant

Tout comme dans le cadre de l'analyse de l'intérêt privé prépondérant, il est de jurisprudence constante qu'un intérêt public prépondérant ne peut être admis qu'avec retenue[478].

L'intérêt public prépondérant tel qu'entendu par cette disposition ne renvoie pas à celui de l'employeur. En effet, l'intérêt public prépondérant doit correspondre à un intérêt de la collectivité publique ou, tout du moins, à celui de plusieurs personnes[479]. Le responsable du traitement peut toutefois faire valoir les intérêts de la collectivité ou d'un groupe de personnes « par substitution »[480].

En droit de la protection des données, le droit de la société à être informée est, en principe, l'intérêt prépondérant public invoqué le plus souvent. Toutefois, il est concevable que d'autres intérêts prépondérants publics soient invoqués par le responsable du traitement afin de justifier le traitement de données envisagé. À titre d'exemple, l'organisateur d'un grand événement sportif peut traiter les données personnelles des participants dans le but de garantir la sécurité de l'événement. Dans la même veine, la mise en œuvre de mesures antidopage (traitement de données médicales des sportifs) contribue à organiser des compétitions sportives justes et équitables[481].

Aucun de ces intérêts ne semble être applicable dans le cadre d'une procédure d'embauche mise en place par un employeur privé. À la lumière de ces exemples et de mon expérience professionnelle, il semble difficile d'imaginer un (autre) intérêt public prépondérant qui pourrait venir justifier le recours au profilage dans le cadre d'une procédure d'embauche entre particuliers.

---

477 ROSENTHAL, Das neue Datenschutzgesetz, N 40.

478 Arrêt du Tribunal administratif fédéral du 18 avril 2017 (A-4232/2015) *Moneyhouse*, cons. 5.4.2.3.

479 NOUREDDINE, pt. 3.130 ; dans le même sens, voir MEIER, Protection des données, N 1612.

480 MEIER, Protection des données, N 1615.

481 WERMELINGER, art. 13 LPD, N 13.

4. Un traitement prévu par la loi

Dans un quatrième temps, un traitement de données contraire à un principe général peut être justifié sur la base d'une loi, qui prévoit le traitement de données litigieux. Or, il n'existe, à l'heure de la rédaction de cette contribution, aucune disposition fédérale (ou cantonale) qui viendrait justifier l'utilisation du profilage dans le contexte d'une procédure d'embauche entre particuliers[482].

Ainsi, ni le premier, ni le troisième ni le quatrième motif justificatif prévus par l'art. 31 LPD ne semblent pouvoir être invoqués pour justifier un profilage dans le cadre d'une procédure d'embauche. Dans certains contextes limités, il n'est pas exclu qu'un intérêt prépondérant privé puisse justifier un profilage. Ces hypothèses devraient pourtant être admises avec *beaucoup* de retenue.

E. L'encadrement de nature technique dépourvu d'effets pratiques

Dans le cadre de la révision de la LPD, le Législateur ne s'est pas contenté d'apporter quelques modifications aux mesures techniques, voire organisationnelles de protection de la personnalité déjà connues sous le régime de l'aLPD. Il a également introduit de nouvelles mesures inspirées du droit européen. Dès lors, il convient de se demander si les mesures prévues aux art. 7, 11, 12 et 13 LPD sont aptes à protéger les droits du candidat lors d'une procédure d'embauche ou si, au contraire, elles sont faciles à contourner par un employeur un peu trop motivé à effectuer un profilage.

1. Les codes de conduite (art. 11 LPD)

L'art. 11 al. 1er LPD fixe que « les associations professionnelles, sectorielles et économiques, lorsqu'elles sont autorisées de par leurs statuts à défendre les intérêts économiques de leurs membres, de même que les organes fédéraux,

482 Il en va autrement dans le cadre des procédures d'embauche dans le secteur public (fédéral). À titre d'exemple, l'Ordonnance sur les contrôles de sécurité relatifs aux personnes (OSCP) du 4 mars 2011, RS 120.4 fixe les traitements de données qui peuvent être effectués à l'égard des personnes figurant à l'Annexe 1. Dans sa version actuelle, il ne semble pas que les consultations des diverses bases de données puissent être qualifiées de « profilage » au sens de la LPD (art. 19 OSCP). Cette constatation est d'ailleurs corroborée par le fait que l'OSCP n'a pas subi de modification dans le cadre de la révision de la LPD, voir FF 2017 6723 ss. ; contrairement au but d'harmonisation poursuivi par le RGPD, le RGPD laisse une certaine marge de manœuvre aux États membres dans la mesure où il serait possible qu'ils adoptent, au niveau national, des dispositions qui prévoient des profilages dans certains contextes, p. ex. en matière de lutte contre le blanchiment d'argent. À ce jour, aucun État membre ne semble avoir adopté une telle disposition ou n'envisage de le faire. Ces mesures nationales dépendront vraisemblablement des efforts de lobbying, voir HÄUSELMANN, N 50. Si cette clause d'ouverture est également pertinente dans le contexte de l'emploi, une loi nationale qui prévoit un profilage au stade de la procédure d'embauche devra prendre en compte les exigences de l'art. 88 RGPD.

peuvent soumettre leur code de conduite au PFPDT » et l'al. 2 précise que « le PFPDT prend position sur les codes de conduite et publie ses prises de position ».

Plusieurs aspects de cette nouvelle disposition – inspirée du RGPD[483] – laissent toutefois penser que son impact en pratique risque d'être modeste.

Ces codes de conduite ne doivent pas impérativement être soumis au PFPDT (bien que le PFPDT ait souhaité la consécration d'une telle obligation dans la nouvelle LPD[484]). Ainsi, reste à savoir si les responsables de traitement feront le choix d'adopter de tels codes de conduite et de les soumettre au PFPDT. Au vu des ressources personnelles limitées du PFPDT, on peut encore se demander s'il a les capacités personnelles de prendre position par rapport aux codes de conduite qui lui auront été soumis sur une base volontaire et s'il est en mesure de se prononcer en temps utile, d'autant plus que la LPD ne fixe aucun délai de réponse, qui pourrait guider les juristes de cette autorité de surveillance dans la gestion des demandes soumises. De surcroît, on notera que même si le PFPDT prend position en temps utile, la LPD ne précise pas les hypothèses dans lesquelles une prise de position serait souhaitable et dans lesquelles, au contraire, il peut se contenter de répondre à la demande en envoyant une lettre de refus standardisée. On notera également qu'une telle prise de position ne constitue pas une décision au sens de l'art. 5 de la Loi fédérale sur la procédure administrative[485] (ci-après « PA »). FÜZESSÉRY et SCHNEIDER estiment ainsi, à juste titre, que les milieux concernés ne peuvent pas en déduire des droits et partir du principe qu'un avis favorable de la part du PFPDT exclut une éventuelle enquête ou des mesures administratives en aval[486]. Cette analyse devra encore faire ses preuves en pratique.

De plus, la LPD prévoit que seules les associations autorisées par leurs statuts à défendre les intérêts économiques de leurs membres peuvent adopter de tels codes de conduite. Une telle réglementation implique que certains responsables de traitement ne seront pas en mesure de fonder leurs traitements

483 Art. 40 et 41 RGPD.

484 Le Conseil fédéral a renoncé à suivre le PFPDT sur ce point, compte tenu des résultats de la consultation externe et parce que le PFPDT aurait dû statuer par voie de décision, ce qui aurait entraîné des coûts supplémentaires, voir FF 2017 6654 ; dans son rapport de 2014, le WEF semble également être d'avis que l'adoption de codes de conduite sur base volontaire ne permet pas d'améliorer la protection des données. En effet, parmi les mesures proposées, les auteurs de ce rapport citent des « codes of conduct *with enforcement* (italique ajouté par mes soins) », voir WEF, p. 22 ; au niveau européen, on rappellera que si le RGPD ne prévoit pas de mesures incitatives, il prévoit toutefois une obligation de soumettre les projets de code de conduite à l'approbation de l'autorité de contrôle compétente et fixe que le suivi d'un tel code de conduite devra être assuré par un organisme externe dûment agréé par une autorité de contrôle (art. 40 al. 5 et 41 RGPD).

485 Loi fédérale sur la procédure administrative du 20 décembre 1968, RS 172.021.

486 FÜZESSÉRY/SCHNEIDER, p. 150.

de données sur de tels codes de conduite faute de faire partie d'une telle association. En d'autres termes, une telle réglementation ne parvient pas à encadrer les traitements de données envisagés par *tous* les employeurs soumis au droit privé.

Enfin on peut se demander si les codes de conduite adoptés par la « partie dominante au contrat » constituent un moyen adéquat pour encadrer l'asymétrie d'information qui prévaut entre l'employeur et le candidat.

En bref, la LPD révisée ne précise ni le délai dans lequel une prise de position sera rendue ni sa portée juridique exacte (p. ex. dans le cadre d'un litige) ni les critères qui guideront les juristes dans la sélection des codes de conduite par rapport auxquels ils souhaiteraient prendre position. On notera qu'en plus de ces incertitudes juridiques, toute prise de position fera l'objet d'une taxe[487] ce qui risque de décourager certains employeurs à s'adresser au PFPDT en amont à un profilage envisagé.

2. La protection des données dès la conception et par défaut (art. 7 LPD)

La protection des données dès la conception (*Privacy by Design*), dont la protection des données par défaut (*Privacy by Default*) constitue un aspect[488], repose sur l'idée que la technologie doit être au service de la protection des données personnelles[489] et que la majorité des violations de la sphère privée ne sont pas détectées[490]. Mesure d'ordre technique par excellence, elle a donc pour but de contribuer à ce que ces violations ne se produisent pas plutôt que de chercher à les sanctionner en aval[491]. Ce concept, initialement développé par CAVOUKIAN puis adopté lors de la 32e Conférence internationale des autorités de la protection des données en 2010[492], soulève néanmoins quelques questions, notamment dans le cadre d'un profilage effectué pendant une procédure d'embauche.

487 Art. 59 al. 1er let. a LPD.

488 De manière convaincante, voir ROSENTHAL, Das neue Datenschutzgesetz, N 43. Au contraire, MÉTILLE ne semble pas se prononcer de manière expresse sur cette question, voir MÉTILLE, L'angle de la (nouvelle) loi, pp. 28 s.

489 Dans son rapport adressé au Conseil de l'Europe, ROUVROY explique les raisons pour lesquelles la plupart des utilisateurs, donc potentiels candidats, sont paresseux lorsqu'il s'agit d'installer des mesures plus protectrices de leurs données personnelles, voir ROUVROY, p. 23.

490 Pour les raisons justifiant cette constatation, voir MÉTILLE, Jurisprudence actuelle, pp. 114 s.

491 MÉTILLE, L'angle de la (nouvelle) loi, p. 28.

492 MÉTILLE, L'angle de la (nouvelle) loi, p. 28 ; pour une analyse plus approfondie et plus critique de ce concept, voir GASSER, p. 379, qui fait également référence aux travaux de RUBINSTEIN à ce sujet ; pour le texte intégral de la résolution de la 32e Conférence internationale des commissaires à la protection des données et de la vie privée, qui reprend les sept principes développés par CAVOUKIAN, voir European Data Protection Supervisor (EDPS), Resolution on Privacy by Design, Jérusalem les 27 au 29 octobre 2010.

Comme relevé à juste titre par TAMÒ-LARRIEUX, la mise en place d'une protection des données dès la conception pose plusieurs problèmes d'un point de vue technique, c'est-à-dire indépendamment du régime juridique qui encadre ces mesures. Ainsi, elle relève des problèmes liés à l'interopérabilité, au défaut d'incitation économique, au développement de systèmes adaptés aux utilisateurs non-professionnels, à l'anonymisation qui devient de plus en plus illusoire et à l'impossibilité d'effacer des données personnelles[493]. Toutes ces observations sont pertinentes tant pour un employeur qui aimerait utiliser un produit développé à la lumière de cette disposition que pour un candidat qui devrait bénéficier d'une certaine protection.

Dans une veine juridique, on notera que la violation de cette disposition ne constitue pas une atteinte à la personnalité au sens de l'art. 30 al. 2 LPD, mais uniquement une violation du devoir de diligence[494]. Cette constatation n'incite pas le sous-traitant à mettre en place une protection des données dès la conception respectivement par défaut la plus efficace possible.

De plus, le choix des mesures concrètes, c'est-à-dire le choix des préréglages mis en place dans un cas d'espèce, est laissé au responsable du traitement[495]. Peu nombreux sont les employeurs qui sont des experts en la matière. Ils resteront donc responsables du traitement, mais devront se fier aux choix librement opérés par le sous-traitant. Ce dernier risque toutefois de ne pas prioriser la mise en place de ces mesures, notamment en raison des faibles conséquences juridiques en cas de violation de cette disposition et de ses intérêts financiers prédominants.

En bref, cette disposition risque de n'avoir qu'une modeste portée en pratique, ce qui sera encore plus vrai lorsque le responsable du traitement ne procède pas lui-même à l'évaluation automatisée et devra, par conséquent, se fier aux choix opérés par son sous-traitant.

3. Les registres des activités de traitement (art. 12 LPD)

L'art. 12 al. 1er LPD prévoit que « les responsables du traitement et les sous-traitants tiennent chacun un registre de leurs activités de traitement ». Si le deuxième alinéa précise le contenu du registre tenu par le responsable du traitement, le troisième alinéa de cette disposition fixe le contenu du registre tenu par le sous-traitant. Le cinquième alinéa prévoit quant à lui une exception de tenir

493 TAMÒ-LARRIEUX, pp. 227 ss.

494 ROSENTHAL, Das neue Datenschutzgesetz, N 43 ; MÉTILLE, L'angle de la (nouvelle) loi, p. 28 ; d'un avis contraire, considérant notamment que la protection des données, dès la conception et par défaut, sont l'expression du principe de proportionnalité (au même titre que le principe de minimisation des données), voir FÜZESSÉRY/SCHNEIDER, p. 149.

495 ROSENTHAL, Das neue Datenschutzgesetz, N 44.

un registre pour les PME qui procèderaient à un traitement qui présente un « risque limité » d'atteinte à la personnalité des personnes concernées.

Cette obligation reprise du droit européen[496] est à saluer dans la mesure où elle contribue à la sensibilisation des responsables du traitement et de leurs éventuels sous-traitants qui sont forcés de se prendre le temps de réfléchir aux traitements envisagés et de les annoter dans un registre[497]. Pour plusieurs raisons, l'impact pratique de cette disposition risque toutefois d'être modeste[498].

La LPD révisée impose cette charge administrative supplémentaire, mais ne prévoit ni l'obligation de soumettre ce registre au PFPDT ni une quelconque sanction si un tel registre fait défaut ou est incomplet[499]. De plus, les personnes concernées par un traitement figurant dans ce registre, comme p. ex. un candidat, n'ont pas accès à ce registre (même s'il est vrai que les informations potentiellement obtenues grâce au droit d'accès ne devraient pas fondamentalement différer de celles qui figurent dans le registre). Seul le PFPDT peut avoir accès au registre des responsables du traitement privés sur demande[500]. Enfin, la portée de l'exception prévue à l'art. 12 al. 5 LPD reste à être déterminée. En effet, si le « risque limité » d'un traitement de données est admis très largement, de nombreux employeurs pourraient faire valoir cette exception vidant ainsi la disposition de son contenu[501].

On retiendra donc que l'art. 12 LPD n'offre guère de garanties supplémentaires à un candidat qui serait soumis à un profilage au stade de la procédure d'embauche. Tout au plus, cette disposition légale contribue à sensibiliser l'employeur et son sous-traitant à la thématique de la protection des données et à répondre plus rapidement à une éventuelle demande d'accès du candidat.

496 Art. 30 RGPD.

497 Dans le même sens, voir ROSENTHAL, Das neue Datenschutzgesetz, N 144.

498 Déjà sous l'aLPD qui prévoyait pourtant une obligation de déclarer les fichiers auprès du PFPDT (art. 11a al. 3-5 aLPD), la portée de cette obligation était modeste, voir, à juste titre, ROSENTHAL, Das neue Datenschutzgesetz, N 143.

499 ROSENTHAL, Das neue Datenschutzgesetz, N 143 et 145.

500 ROSENTHAL, Das neue Datenschutzgesetz, N 145 ; MÉTILLE, L'angle de la (nouvelle) loi, p. 16. On notera que contrairement aux registres tenus par les privés, les registres des organes fédéraux sont publiés (art. 56 LPD). Certains spécialistes ont même fait valoir que la publication des registres tenus par des privés permettrait tant aux personnes concernées (comme p. ex. les consommateurs de services ou des candidats) qu'aux autorités de surveillance de vérifier quelles données sont traitées à quelles fins. Ainsi, il est regrettable que le Législateur ait opté d'abolir l'obligation de déclarer les fichiers (certes peu efficace dans sa forme prévue sous l'aLPD) au lieu de la renforcer, voir, à titre d'exemple et avec des références supplémentaires, CHRISTL/SPIEKERMANN, p. 143.

501 L'incertitude qui entoure les notions de « risque limité » et « risque élevé » a un effet sur l'application de plusieurs dispositions de la LPD. Il découle de cette constatation que tant le Tribunal fédéral que le PFPDT sont appelés à interpréter ces notions à la lumière du cadre constitutionnel pertinent dans ce contexte, voir *infra* Chapitre 11. Le cadre constitutionnel suisse.

4. Les certifications (art. 13 LPD)

Mesure d'autorégulation entrée en vigueur en 2008 dans le cadre d'une révision partielle de l'aLPD[502], l'art. 11 aLPD fixait le cadre d'une évaluation facultative des systèmes, des procédures et des organisations[503]. Le nouvel art. 13 al. 1er LPD fixe que « les fournisseurs de systèmes ou de logiciels de traitement de données personnelles ainsi que les responsables du traitement et les sous-traitants peuvent soumettre leurs systèmes, leurs produits ou leurs services à une évaluation effectuée par des organismes de certification agréées et indépendants » et n'apporte ainsi qu'une modification modeste à l'art. 11 aLPD[504]. Ainsi, les critiques qui ont pu être mises en avant sous l'aLPD par rapport aux certifications sont toujours pertinentes[505].

Il découle de la lettre de la disposition légale que, tout comme l'aLPD, la nouvelle LPD n'impose aucune obligation de soumettre le traitement de données à une quelconque certification. Comme l'obligation de tenir un registre de certains traitements de données, la certification constitue une mesure d'autorégulation facultative, qui n'a eu qu'une portée modeste par le passé[506]. En effet, sous le régime de l'aLPD, les responsables de traitement procédaient à une

502 FF 2003 1915.

503 Les détails de cette évaluation étaient fixés dans l'Ordonnance sur les certifications en matière de protection des données (aOCPD) du 28 septembre 2007, remplacée par l'Ordonnance sur les certifications en matière de protection des données (OCPD) du 31 août 2022, RS 235.13 (entrée en vigueur fixée au 1er septembre 2023).

504 En vertu de la nouvelle LPD, il est désormais possible de faire certifier non seulement des systèmes (procédures et organisations) et des produits (programmes, logiciels, systèmes), mais aussi des services, voir FF 2017 6656.

505 Il convient toutefois de noter que les contours de l'art. 13 LPD ont été fixés dans l'OCPD révisée du 31 août 2022, pour des précisions quant aux quelques modifications ponctuelles apportées au régime des certifications dans le cadre de la révision de la LPD, voir Office fédéral de la justice (OFJ), Domaine de direction Droit public, Ordonnance sur les certifications en matière de protection des données (OCPD), Rapport explicatif du 31 août 2022.

506 Pour une appréciation sans équivoque de cet outil d'autorégulation sous l'aLPD, voir UTTINGER, pp. 77 ss., qui précise qu'« [traduction] une entreprise certifiée [...] ne doit pas nécessairement prendre au sérieux le thème de la protection des données. Il est – malheureusement – possible qu'une entreprise obtienne une certification sans vraiment mettre en œuvre des mesures efficaces de protection des données et sans les prendre au sérieux en tant qu'élément de la gouvernance de l'entreprise, au même titre qu'une entreprise non-certifiée » et qui, un peu plus loin, tranche en affirmant, à juste titre, qu' « [traduction] une telle certification n'est pas le bon moyen pour améliorer la protection des données » (*ob eine solche Zertifizierung der richtige Weg ist, um den Datenschutz zu verbessern, ist zu verneinen*).

certification uniquement lorsqu'elle était prévue par une loi[507], qu'elle était obligatoire dans le cadre d'appels d'offre ou que le responsable espérait en tirer un avantage concurrentiel[508]. Rien ne laisse penser que cette constatation ne serait plus pertinente sous le régime de la nouvelle LPD.

Dans ce contexte, on rappellera que le PFPDT aurait souhaité rendre la certification obligatoire pour les profilages à risque élevé[509]. Étant donné qu'une telle mesure n'est pas prévue en droit européen, cette proposition a été rejetée par le Conseil fédéral[510]. Ainsi, force est de constater qu'aucune disposition applicable au stade de la procédure d'embauche ne fixe que de telles évaluations automatisées des candidats doivent avoir été certifiées au préalable. Si le Conseil fédéral ne souhaitait pas trop étendre l'obligation de certifier certains traitements, il aurait pu songer à prévoir une telle obligation non pas dans la LPD applicable à tous les traitements entre privés, mais dans des lois spéciales qui régissent certaines relations juridiques particulièrement sensibles. Pour les traitements effectués pendant la relation précontractuelle de travail, une telle obligation aurait pu être prévue à l'art. 328b CO, voire dans un nouvel art. 328c CO (ce qui n'aurait d'ailleurs que confirmé l'approche préconisée sous l'aLPD[511]). Comme mentionné plus haut, la pratique a pu montrer que sans obligation légale de procéder à une certification d'un traitement envisagé, peu de responsables de traitement optent pour une certification.

De plus, certaines entreprises accréditées par le Service d'accréditation suisse[512] offrent certes de telles certifications. Au vu de leur prix et de leur faible visibilité en pratique, elles sont toutefois uniquement accessibles aux grandes entreprises qui disposent de moyens financiers conséquents et attachent une certaine importance à la protection des données.

Enfin, on rappellera qu'une certification porte toujours sur une évaluation de traitements effectués dans le passé. Or, même si l'évaluation est positive,

507 À titre d'exemple, on pensera à l'art. 59a al. 6 de l'Ordonnance sur l'assurance-maladie (OAMal, RS 832.102) qui prévoit que pour la facturation dans le cas d'un modèle de rémunération de type DRG, les assureurs doivent disposer d'un service de réception des données certifié.

508 ROSENTHAL, Das neue Datenschutzgesetz, N 179.

509 Pour les raisons pour lesquelles un profilage effectué pendant la procédure de recrutement devrait être qualifié, dans la plupart des cas, de « profilage à risque élevé », voir *supra* Chapitre 8. La Loi sur la protection des données.

510 FF 2017 6656. Cette décision n'a rien d'étonnant dans la mesure où le droit européen ne connaît pas le profilage à risque élevé.

511 À titre d'exemple, on pensera à l'art. 59a al. 6 OAMal cité plus haut.

512 La procédure d'accréditation des organismes de certification indépendants par le Service d'accréditation suisse, à laquelle le PFPDT est associé, n'a pas subi de modification dans le cadre de la révision, voir FF 2017 6656.

il n'est pas garanti que l'application du programme utilisé permettra d'atteindre le but poursuivi par le responsable du traitement dans de nouveaux contextes avec de nouvelles données. Ainsi, un régime juridique efficace en la matière devrait également prévoir des mesures de supervision de l'utilisation de ces programmes[513].

Cela étant, si le cadre légal imposait certaines obligations aux responsables de traitement et que les certifications acquerraient une visibilité suffisante au sein de la société civile[514], les certifications pourraient avoir un impact important en pratique. On pensera, à titre d'exemple, au label « Swiss LGBTI » qui est un label de qualité octroyé aux organisations basées en Suisse ou aux organisations suisses qui œuvrent pour l'égalité des personnes LGBTI au sein des entreprises[515], aux certifications énergétiques[516] ou encore au label « AOC » qui permet d'identifier un produit dont les étapes de fabrication sont réalisées dans une même zone géographique et selon un savoir-faire reconnu. Imposer une certification uniforme aurait pour effet secondaire bénéfique de standardiser la protection des données au stade de la procédure d'embauche[517] et de contribuer à éviter des détournements des protections légales[518]. Dans sa forme actuelle cependant, cette mesure d'autorégulation ne contribue pas à améliorer la protection des droits des candidats et doit être qualifiée de superflue[519].

5. Les analyses d'impact (art. 22 et 23 LPD)

Dans le cadre de la révision, le Législateur suisse s'est inspiré du droit européen[520] et a introduit l'analyse d'impact relative à la protection des données

513 AlgorithmWatch, p. 33.

514 Dans le même sens, voir UTTINGER, p. 77.

515 Swiss LGBTI Label, Plus de succès grâce au Swiss LGBTI-Label, Swiss LGBTI-Label : qu'est-ce que c'est et en quoi est-ce utile?, publication non-datée.

516 HIRSCH, pp. 60 ss.

517 Pour un aperçu critique des multiples certifications supplémentaires en matière de protection des données, voir UTTINGER, pp. 76 s. Une telle « cacophonie de certifications » ne contribue pas à une amélioration de la protection des données, bien au contraire.

518 Un des défis majeurs de la protection des données à l'ère numérique est en effet que les données peuvent être collectées n'importe où dans le monde, à n'importe quel moment, par n'importe qui avant d'être transmises à n'importe quel endroit. En d'autres termes, contourner un régime légal national devient très simple. Une standardisation, du moins de certaines mesures, contribuerait à garantir un niveau minimal de protection indépendamment du lieu du traitement de données, voir, dans le même sens, RGPD, considérants 6 et 10 et Convention 108+, pt. 3 et son Préambule.

519 Dans le même sens déjà à propos du régime prévu sous l'aLPD, voir UTTINGER, p. 80. Elle précise qu'« ainsi, la loi suisse sur la protection des données est une loi sans effets et l'art. 11 [aLPD] une disposition superflue » (*so bleibt das schweizerische Datenschutzgesetz ein zahnloses Gesetz und Art. 11 ein überflüssiger Artikel*).

520 Art. 35 RGPD et art. 10 al. 2 Convention 108+ respectivement.

en droit suisse. « Il s'agit d'un outil préventif à destination du responsable du traitement qui devrait lui permettre, après avoir décrit le traitement qu'il entend mettre en œuvre, d'en évaluer la nécessité et la proportionnalité tout en évaluant les risques pesant sur les droits et libertés des personnes physiques au vu du traitement envisagé »[521]. En cas de risque élevé pour lesdits droits et libertés, le responsable du traitement doit déterminer les mesures nécessaires pour y faire face.

Tout comme l'obligation de tenir un registre des traitements effectués, les analyses d'impact telles que définies à l'art. 22 al. 3 LPD ont l'avantage de contribuer à la sensibilisation des responsables du traitement[522] et permettent d'anticiper d'éventuels problèmes juridiques liés à la protection des données[523]. Pour plusieurs raisons, l'impact pratique de ces analyses risque toutefois d'être limité.

D'abord, la notion de « risque élevé » dans le contexte d'un profilage n'est que peu claire, notamment en raison de la décision du Législateur d'éliminer, au dernier moment[524] et contrairement à ce qui a pu être prévu en droit européen[525], le profilage « général » de la liste des traitements de données à risque. Cette décision est regrettable dans le contexte de la procédure d'embauche dans la mesure où un profilage effectué sans la mise en place de mesures protectrices des droits du candidat peut priver ce dernier d'accéder au marché du travail et donc porter atteinte à plusieurs droits et libertés dudit candidat. À défaut de plus de clarté quant aux traitements à risque élevé, le responsable du traitement qui procède à un profilage devra « faire un lien entre, d'une part, le traitement envisagé et, d'autre part, le droit à l'autodétermination informationnelle de la personne concernée ainsi que son droit à sa sphère privée. Il s'agit donc de prendre en considération le traitement des données au regard de l'autodétermination, de l'identité et de la dignité de la personne concernée »[526].

521 MÉTILLE, L'angle de la (nouvelle) loi, p. 22.

522 Pour une analyse plus approfondie de l'importance de la sensibilisation des responsables de traitement et de leurs sous-traitants à la protection des données, voir *infra* Chapitre 15. Résumé des propositions.

523 FF 2017 6676.

524 Au sujet du projet de l'art. 22 al. 2 let. b, le Message précise « qu'un risque élevé existe en cas de profilage. Tel peut être également le cas lorsque des décisions sont prises exclusivement sur la base d'un traitement de données personnelles automatisé, y compris en cas de profilage, et que ces décisions ont des effets juridiques sur la personne concernée ou l'affectent de manière notable. Il ne faut pas perdre de vue en effet que ce type de décisions peuvent, selon le cas, avoir des répercussions non négligeables pour la personne concernée », voir FF 2017 6677.

525 Art. 35 al. 3 let. a RGPD. On précisera toutefois que l'analyse d'impact n'est obligatoire uniquement si le profilage est suivi d'une décision individuelle automatisée.

526 FF 2017 6677.

Pour les raisons identifiées plus haut, un alignement du risque élevé tel que mentionné à l'art. 22 LPD sur la définition du « profilage à risque élevé » figurant à l'art. 5 let. g LPD ne conduit pas à des résultats satisfaisants[527]. Une évaluation au cas par cas sur la base des éléments mentionnés dans le Message[528] (et potentiellement d'éléments supplémentaires) est alors de mise ce qui engendre une insécurité juridique supplémentaire.

Il convient toutefois de noter que même s'il est admis qu'un profilage effectué dans le cadre d'une procédure d'embauche représente un risque qui justifie une analyse d'impact, la nouvelle LPD prévoit trois exceptions importantes qui permettent au responsable du traitement de renoncer à une telle analyse. D'une part, une analyse d'impact n'est pas de mise lorsque le traitement est effectué sur la base d'une obligation légale (exception non-applicable dans l'hypothèse d'un profilage effectué dans le cadre d'une procédure d'embauche régie par le droit privé). D'autre part, le responsable ne devra pas effectuer une telle analyse si le traitement envisagé a été certifié au sens de l'art. 13 LPD. Enfin, l'obligation de procéder à une analyse d'impact peut être contournée dans les cas où le responsable a adopté un code de conduite. Comme nous l'avons vu plus haut déjà, il n'est pas certain qu'une certification ou qu'un code de conduite soit en mesure de garantir le respect des droits et libertés d'un candidat soumis à un profilage. En d'autres termes, ces exceptions risquent de considérablement restreindre l'impact pratique de ce nouvel instrument d'autorégulation, dont la mise en œuvre peut être évitée par la mise en place d'autres mesures peu efficaces.

Enfin, on rappellera que si le responsable du traitement conclut, après avoir procédé à l'analyse, que le traitement comporte encore un risque pour les droits des personnes concernées, il doit consulter le PFPDT[529]. Il va sans dire que la plupart des responsables souhaiteront contourner cette intervention de l'autorité de surveillance[530] (intervention qui coûtera en temps et dont le contenu, de surcroît, est peu prévisible, compte tenu que la LPD est restée très vague au sujet de cette intervention) et auront donc la tendance d'admettre un peu

527 Voir *supra* Chapitre 8. La Loi sur la protection des données.

528 Le Conseil fédéral précise, à ce sujet, qu'« on peut admettre l'existence d'un risque élevé lorsqu'il apparaît que les propriétés du traitement envisagé ont – ou pourraient avoir – pour effet de restreindre dans une large mesure la liberté de la personne de disposer de ses données. Ce risque élevé peut résulter, par exemple, de la nature ou du contenu des données à traiter […], de la nature ou de la finalité du traitement envisagé (p. ex. profilage), de la quantité de données à traiter, de leur transmission vers un État tiers […] ou de ce que les données seraient accessibles à un grand nombre, voire à un nombre illimité, de personnes », voir FF 2017 6677.

529 Art. 23 al. 1er LPD.

530 Pour des réserves émises, à juste titre, quant à la portée de ces analyses en pratique, voir ROSENTHAL, Das neue Datenschutzgesetz, N 154 s.

trop facilement que le traitement envisagé ne risque ni de porter atteinte à l'autodétermination de la personne concernée, ni à sa dignité ni à son identité[531].

Contrairement à ce qui a pu être fixé en droit européen[532] et dans le projet de loi[533], une analyse d'impact n'est pas expressément requise en cas de profilage et l'omission de procéder à une telle analyse (dans les cas prévus par le droit suisse) n'est pas sanctionnée par une amende[534]. Une telle omission ne constitue ni une atteinte à la personnalité au sens de l'art. 30 al. 2 LPD ni une violation d'un des devoirs de diligence définis à l'art. 61 LPD. Une analyse d'impact ne peut pas non plus être imposée par voie judiciaire sur demande de la personne concernée, p. ex. un candidat soumis à un profilage ; seul le PFPDT peut l'ordonner[535] ce qui ne sera, en pratique, probablement que rarement le cas[536].

En conclusion, on retiendra donc qu'en raison de l'incertitude qui entoure la notion de « risque élevé » dans le cadre d'un profilage, des exceptions prévues à l'obligation de procéder à une analyse d'impact et de l'absence d'une quelconque sanction en cas d'omission d'une telle analyse, ce nouvel instrument ne contribue pas ou que très modestement à une meilleure protection des droits des candidats.

F. Une protection insuffisante

Il découle de ce qui précède que la LPD n'encadre le profilage effectué dans le contexte d'une procédure d'embauche que de manière insatisfaisante. D'abord, plusieurs éléments de la définition du profilage et du profilage à risque élevé sont peu clairs et devront être clarifiés par les tribunaux. On pensera aux contours vagues des notions constitutives du profilage, notamment celle de « donnée personnelle » et celle de « traitement entièrement automatisé » ainsi qu'au flou qui entoure le but d'un tel traitement de données. La notion de « risque élevé » quant à elle suscite de nombreuses questions auxquelles il peut être répondu de manière très divergente. Dans une veine similaire, la distinction

531 FF 2017 6677.

532 Art. 35 al. 3 let. a RGPD.

533 FF 2017 6677.

534 En droit européen, la violation de cette obligation fait l'objet d'amendes administratives pouvant s'élever jusqu'à 10'000'000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, voir l'art. 83 al. 4 let. a RGPD.

535 Le PFPDT peut soit ordonner que le responsable privé procède à une analyse d'impact soit, si une telle analyse a déjà été effectuée et a montré que le risque de violation des droits de la personne concernée est élevé, de le consulter, voir l'art. 51 al. 3 let. d et e LPD.

536 Malgré une augmentation des effectifs du PFPDT, il n'en demeure pas moins que la taille de l'autorité de surveillance reste modeste.

entre les deux formes de profilage d’une part et entre un profilage (général ou à risque élevé) et une décision individuelle automatisée d’autre part ne pourront être clarifiées de manière contraignante que par le pouvoir judiciaire.

Les principes généraux tels que consacrés aux art. 6 et 8 LPD ainsi que les motifs justificatifs tels que fixés à l’art. 31 LPD sont, d’une manière générale, utiles en matière de protection des données. En effet, ce régime offre une certaine flexibilité face aux développements de nouveaux traitements de données et garantissent une solution appropriée au cas par cas. Toutefois, dans l’hypothèse d’un profilage effectué pendant une procédure d’embauche, les principes de proportionnalité et de finalité sons systématiquement violés, notamment en raison de l’incertitude liée aux questions de savoir si un profilage est apte à recruter le meilleur candidat et s’il est raisonnable d’opposer le comportement d’une personne tierce au candidat qui, pour des raisons qu’il ignore, partage certaines caractéristiques avec ces tiers inconnus. Une violation des autres principes généraux est également concevable, même si elle ne sera probablement pas retenue dans tous les cas de figure. Une violation d’un principe général supplémentaire devra être relevée lorsqu’un profilage est effectué à l’insu du candidat (violation du principe de la transparence, voire violation du principe de la bonne foi) ou lorsque l’évaluation proposée par le profilage s’avère inexacte (violation du principe d’exactitude).

En droit suisse, une violation d’un principe général peut être justifiée si le responsable du traitement est en mesure d’invoquer un des quatre motifs justificatifs prévus par la LPD. En raison du lien de subordination qui, selon une majorité de la doctrine, caractérise la relation entre l’employeur et le candidat, ce dernier ne saurait librement consentir au traitement de données envisagé (on rappellera également qu’en vertu d’une lecture restrictive des art. 328b et 362 CO, le candidat ne saurait consentir à un traitement de données qui irait au-delà de ce qui est « nécessaire » tel qu’entendu par l’art. 328b CO). L’intérêt privé prépondérant de l’employeur qui sera (le plus souvent) de nature économique ne semble pas être en mesure de justifier un traitement de données qui a le potentiel de rendre le candidat transparent. Dans le cadre d’une procédure d’embauche soumise au droit privé, ni une loi ni un quelconque intérêt public prépondérant ne saurait être invoqué. En bref, un profilage effectué dans le cadre d’une procédure d’embauche viole systématiquement les droits de la personnalité tels que protégés par la LPD. Ce constat n’a rien d’étonnant dans la mesure où les principes généraux n’ont pas été conçus pour encadrer un traitement de données fondés sur un calcul de corrélations[537].

537 Dans le même sens à propos du principe de finalité (et du devoir d’informer et du consentement), voir MEIER, Big Data, p. 91.

S'il est impératif d'appréhender les défis identifiés en adoptant une approche pluridisciplinaire, force est de constater que les moyens juridiques prévus par la LPD n'offrent guère de protection au candidat.

Les diverses mesures d'ordre technique risquent de n'avoir qu'un impact très modeste en pratique, notamment en raison de leur caractère facultatif[538], des moyens juridiques et personnels restreints du PFPDT[539] et d'un manque de sensibilisation des responsables de traitement. En d'autres termes, ces mesures ne contribueront pas à l'amélioration de la protection des droits des personnes concernées. Elles n'alourdissent uniquement les obligations administratives qui pèsent sur les employeurs.

Dans sa version révisée, la LPD laisse le soin aux personnes concernées de s'opposer à un traitement de leurs données qu'elles estiment contraire à leurs droits. Une opposition à un traitement de données (principe du *opt-out*) présuppose toutefois que la personne concernée ait connaissance du profilage (ce qui n'est pas toujours le cas) et qu'elle fasse preuve d'un certain courage. Une telle opposition est encore plus compliquée dans une relation de subordination. Cette constatation est d'autant plus vraie que le profilage est actuellement avant tout effectué dans des secteurs qui occupent des personnes souvent peu qualifiées et donc – faute de vrai choix sur le marché de l'emploi – potentiellement plus enclines à accepter des traitements de données contraires à leurs propres intérêts. Les actions en justice en matière de protection des données étaient rares sous le régime de l'aLPD. Aucune disposition dans la LPD ne laisse penser qu'il en sera différemment sous le régime de la LPD révisée. Ainsi, les insécurités juridiques liées aux différentes définitions légales telles qu'identifiées ne seront très probablement pas adressées par les juges de sitôt. Face au profilage effectué dans le cadre d'une procédure d'embauche, un encadrement plus strict et plus clair aurait donc eu l'avantage d'augmenter la sécurité juridique et de mieux garantir les droits des candidats concernés. Dès lors, reste à savoir si la Suisse devrait s'inspirer du cadre légal européen afin de combler les lacunes identifiées ci-dessus.

538 Pour une analyse des raisons économiques pour lesquelles les mesures d'autorégulation facultatives restent sans effets, voir ZUBOFF, Surveillance Capitalism, p. 248.

539 Dans son rapport d'activités actuel, le PFPDT précise qu'il « ne dispose pas de moyens suffisants pour effectuer des contrôles aléatoires et systématiques de la sécurité technique qu'exigent pourtant les bases de données sensibles », voir PFPDT, 29e Rapport d'activités, p. 10.

G. Digression : le droit européen – une source d'inspiration ?

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD ») est directement applicable depuis le 25 mai 2018 dans tous les États membres de l'Union européenne[540] (ci-après « UE »). Le RGPD a remplacé la Directive 95/46/CE sur la protection des données personnelles du 24 octobre 1995 (ci-après « DPD »). S'il est vrai que la DPD avait pour but de protéger les libertés et les droits fondamentaux des personnes physiques, notamment leur vie privée, elle visait, avant tout, à garantir la libre circulation des données à caractère personnel au sein de l'UE, notamment à des fins commerciales[541]. S'agissant d'une Directive, les États membres jouissaient d'une certaine marge de manœuvre lors de sa mise en œuvre. Ainsi, certains États avaient mis en place des mécanismes plus stricts que ceux prévus dans la DPD, d'autres, au contraire, avaient adopté un régime plus souple que celui prévu en droit européen, la DPD n'ayant donc pas pu éviter une certaine fragmentation (et donc une certaine insécurité juridique) des régimes nationaux relatifs à la protection des données[542].

Le RGPD quant à lui poursuit deux buts. D'une part, le RGPD vise à offrir aux personnes physiques une protection unifiée de leurs libertés et droits fondamentaux au sein de l'UE et, en particulier, de leur droit à la protection des données à caractère personnel[543]. D'autre part, le RGPD a pour but de garantir la libre circulation des données à caractère personnel au sein de l'UE. Cette libre circulation ne saurait être ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[544]. Si à première vue ces deux buts peuvent sembler contradictoires, cette contradiction ne serait due qu'à une rédaction maladroite de l'art. 1er RGPD[545]. En effet, ces deux buts ne s'excluent pas, mais, au contraire, se complètent : « Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres »[546].

540 Art. 99 al. 2 RGPD.
541 Art. 1er DPD.
542 Considérant 9 RGPD.
543 Art. 1er al. 2 RGPD.
544 Art. 1er al. 3 RGPD.
545 SYDOW, art. 1er RPGD, N 2 s.
546 Considérant 10 RGPD.

On rappellera que l'art. 29 DPD instaurait le « Groupe de protection des personnes à l'égard du traitement des données à caractère personnel » (ci-après « Groupe de travail 'Article 29' »), qui avait pour vocation de publier des prises de position dans le but d'unifier le droit de la protection des données en Europe. Ce groupe de travail indépendant était composé des représentants des autorités nationales de protection des données, d'un représentant de l'autorité créée pour les institutions et organismes communautaires et d'un représentant de la Commission européenne. Avec la mise en œuvre du RGPD, ce groupe de travail a été remplacé par le Comité européen de la protection des données qui possède la personnalité juridique et se compose du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données[547]. Ainsi, tout comme la jurisprudence pertinente de la CJUE[548], les publications du Groupe de travail « Article 29 » et de son organe successeur doivent être prises en compte lors de toute analyse des dispositions européennes en matière de protection des données.

Au vu des développements technologiques, l'adoption d'une définition légale du profilage ainsi qu'un encadrement de ce nouveau traitement de données s'imposaient dans le cadre des travaux de révision de la DPD[549]. Ainsi, il convient de se pencher sur la définition du profilage consacrée à l'art. 4 ch. 4 RGPD (1) avant d'examiner le cadre légal du profilage en droit européen à la lumière des deux buts affichés par le Législateur européen lors de l'adoption du RGPD (2).

1. La définition problématique du profilage en droit européen (art. 4 ch. 4 RGPD)

En guise de rappel, il convient de noter que l'art. 4 ch. 4 RGPD définit le profilage comme étant « toute forme de traitement automatisé de données à caractère

547 Art. 68 ss. RGPD.

548 Si cette précision est certes pertinente en théorie, on notera qu'à la fin septembre 2022, aucune décision n'a été rendue par la CJUE quant aux contours exacts de la notion de profilage. Seules les conclusions de l'Avocat général du 27 janvier 2022 portent, entre autres, sur le cadre à prévoir lorsqu'un profilage est envisagé. De plus, il convient de noter que la demande de renvoi préjudiciel qui a été adressée à la CJUE en amont à ces conclusions ne concernait pas directement la notion de profilage telle que consacrée dans le RGPD, mais celle (identique) prévue dans la Directive (UE) 2016/681 du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, voir CJUE, 27 janvier 2022, *Conclusions de l'avocat général de la Cour*, C-817/19, pt. 223 ss. Dans son arrêt du 21 juin 2022, la CJUE prend certes note des développements de l'Avocat général relatifs au profilage et rappelle quelques risques liés à ce traitement de données, mais ne s'attarde pas sur cette notion et conclut que la Directive 2016/681 est conforme aux art. 7 et 8 Charte, voir CJUE, 21 juin 2022, *C-817/19*, pt. 85 ss.

549 HÄUSELMANN, N 11.

personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail (...) »[550]. Deux différences par rapport au droit suisse méritent d'être soulevées : D'une part, le RGPD utilise la notion de « données à caractère personnel » au lieu de « données personnelles ». Cette différence n'a aucune implication en pratique. Les deux notions sont synonymes[551]. D'autre part, le droit européen ne connaît pas la notion de « profilage à risque élevé ». En d'autres termes, cette notion est une spécificité suisse (et depuis peu du « droit » du Conseil de l'Europe) analysée plus haut déjà[552]. Ainsi, en raison des définitions légales identiques, les analyses de la définition européenne du profilage sont également intéressantes lorsqu'il s'agit de circonscrire le cadre exact à donner au profilage en droit suisse.

D'abord, il convient de déterminer ce qui doit être entendu par « traitement automatisé ». Comme en droit suisse, on peut se demandersi la définition couvre uniquement les traitements *entièrement* automatisés[553] ou si, au contraire, elle englobe également les traitements que *partiellement* automatisés, c'est-à-dire les traitements de données dans le cadre desquels une personne physique peut influencer un aspect du traitement. Les Lignes directrices du Groupe de travail « Article 29 » sont claires à ce sujet : « le profilage doit impliquer une certaine forme de traitement automatisé – bien que la participation humaine n'exclue pas nécessairement l'activité de la définition »[554]. Ainsi, contrairement à ce qui a pu être fixé quant à la décision individuelle automatisée[555], un traitement de données ne doit pas être entièrement automatisé afin de tomber dans le champ d'application de l'art. 4 ch. 4 RGPD. En d'autres termes, il suffit que le traitement de données ne soit pas entièrement effectué à la main pour être considéré un traitement de données automatisé[556]. Sur ce point, la définition européenne est donc plus large que celle retenue en droit suisse.

550 Pour une comparaison détaillée entre la définition européenne et suisse, voir *supra* Chapitre 2. La définition compliquée du profilage.

551 À cette fin, on comparera la lettre de l'art. 5 let. a LPD et celle de l'art. 4 ch. 1er RGPD.

552 Voir *supra* Chapitre 2. La définition compliquée du profilage.

553 On rappellera que le Message précise à ce titre qu'« on est [...] en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé », voir FF 2017 6642. Pour une analyse critique de cette lecture stricte de ce premier élément constitutif du profilage en droit suisse, voir *supra* Chapitre 8. La Loi sur la protection des données.

554 Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 7.

555 Art. 22 al. 1er RGPD.

556 SCHOLZ, art. 4 ch. 4 RGPD, N 3.

Ensuite, il s'agit de savoir dans quelle mesure les traitements automatisés de données anonymes tombent dans le champ de la définition du profilage en droit européen. En effet, tout comme la LPD, le RGPD précise que le profilage est un traitement de données à caractère personnel. Dans ce contexte, il convient de relever une contradiction entre les Lignes directrices du Groupe de travail « Article 29 » et le RGPD. En effet, le Groupe de travail « Article 29 » estime, notamment en se fondant sur la Recommandation CM/Rec(2010)13 du Comité des Ministres[557], que le profilage est constitué de trois traitements de données distincts qui sont effectués les uns après les autres : une collecte de données (à caractère personnel *ou* anonymes), une analyse automatisée afin d'établir des corrélations (entre ces données à caractère personnel *ou* anonymes) et l'application de la corrélation à une personne pour déduire les caractéristiques du comportement actuel ou futur[558]. Or, la définition susmentionnée du RGPD ne couvre ni la collecte de données anonymes ni le calcul de corrélations entre ces données anonymes (les deux premières étapes potentielles d'un profilage)[559]. La définition retenue n'intègre pas les précisions figurant dans l'Exposé des motifs relatif à cette Recommandation du Comité des Ministres. En effet, le Comité des Ministres encourage les responsables de traitement à traiter les données anonymes avec un certain cautionnement[560]. Dans une veine similaire, HÄUSELMANN relève que cette référence à la Recommandation du Conseil de l'Europe est problématique dans la mesure où la simple collecte de données ne semble pas tomber dans le champ d'application de l'art. 4 ch. 4 RGPD (alors qu'elle constitue la première étape du processus du profilage pour le Comité des Ministres)[561].

557 On rappellera que cette Recommandation qui date de 2010 a été révisée. Dans le cadre de cette révision, la définition du profilage a été revue en profondeur. Une Recommandation révisée a été publiée en novembre 2021 (Recommandation CM/Rec[2021]8).

558 Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, pp. 7 s. ; pour de plus amples développements quant au processus de profilage, voir *supra* Chapitre 2. La définition compliquée du profilage.

559 À ce sujet, SCHOLZ mentionne le risque de ré-identification de plus en plus important sans pour autant en déduire une quelconque conséquence quant au champ d'application matériel de cette disposition, voir SCHOLZ, art. 4 ch. 4 RGPD, N 3 ; voir, pour plus de détails quant à ce risque de ré-identification, *supra* Chapitre 2. La définition compliquée du profilage et Chapitre 5. Avantages et risques.

560 Exposé des motifs relatifs à la Recommandation profilage 2010, pt. 99.

561 HÄUSELMANN précise que « [traduction] cette affirmation [la description des trois étapes distinctes du profilage en vertu des Lignes directrices sur la prise de décision individuelle automatisée et le profilage] peut prêter à confusion. Il est évident que la définition du profilage telle que fixée dans le RGPD implique plus que la simple collecte de données personnelles dans le but de les évaluer ultérieurement. Le terme ‹utilisation des données› (*use of data*) suggère que l'évaluation doit être en cours pour [que le traitement puisse] constituer un profilage », voir HÄUSELMANN, N 5 ; pour d'autres auteurs qui distinguent entre la collecte des données et leur évaluation ultérieure, voir SCHWARTMANN/HERMANN, art. 4 ch. 4 RGPD, N 56.

De plus, on relèvera que le troisième élément de la définition prévoit que le but d'un profilage consiste à évaluer certains aspects de la personnalité d'une personne physique sur la base d'un processus automatisé. En d'autres termes, le profilage est un traitement de données qui vise à générer de nouvelles connaissances. À cette fin, une donnée personnelle n'est pas consultée comme telle, mais est interprétée seule ou en combinaison avec d'autres données personnelles. Ainsi, comme en droit suisse, la simple vérification d'une information ne constitue pas un profilage au sens de l'art. 4 ch. 4 RGPD[562].

En outre, le quatrième élément de la définition fixe que l'évaluation doit porter sur certains aspects de la personnalité de la personne concernée. On notera que la liste de ces aspects est non-exhaustive[563] ce qui implique une interprétation large de ce quatrième élément[564]. De plus, aucun critère clair ne fixe combien d'aspects doivent être analysés afin que l'analyse puisse tomber dans le champ de la définition[565]. Ainsi, opérer la distinction entre une donnée à caractère personnel et une information relative à un aspect personnel peut s'avérer compliquée dans la mesure où une (seule) donnée à caractère personnel peut révéler un aspect de la personnalité de la personne concernée (à titre d'exemple, on pensera aux données biométriques). Cet élément ne permet donc pas de procéder à une délimitation claire entre un traitement de données « général » et un profilage[566]. L'élément clé de la définition est donc le troisième élément. En d'autres termes, la question centrale à se poser est celle de savoir si le traitement de données envisagé constitue une évaluation au sens de l'art. 4 ch. 4 RGPD ou pas[567].

562 SCHOLZ, art. 4 ch. 4 RGPD, N 6 ; pour un autre exemple de traitement de données qui peut, selon les circonstances, être qualifié de profilage, voir Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 7.

563 ESSER, art. 4 ch. 4 RGPD, N 66 ; SCHWARTMANN/HERMANN, art. 4 ch. 4 RGPD, N 54 ; HERBST/BUCHNER, art. 4 ch. 4 RGPD, N 7 ; pour des précisions moins explicites quant à la nature de cette énumération, voir Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, pp. 7 s.

564 HERBST/BUCHNER, art. 4 ch. 4 RGPD, N 7 ; SCHOLZ, art. 4 ch. 4 RGPD, N 4 ; pour des exemples supplémentaires d'« aspects de la personnalité des personnes concernées », voir ARNING/ROTHKEGEL, art. 4 ch. 4 RGPD, N 112.

565 À juste titre, SCHOLZ rappelle qu'une évaluation d'une quantité plus importante de données n'entraîne pas nécessairement un risque plus élevé pour les droits des personnes concernées. La forme plurielle (*certains aspects personnels*) semble uniquement indiquer que le profilage doit, au moins, porter sur l'évaluation de deux données personnelles distinctes, voir SCHOLZ, art. 4 ch. 4 RGPD, N 5.

566 SCHOLZ, art. 4 ch. 4 RGPD, N 4 ; pour des développements allant dans le même sens à propos de la définition suisse, voir *supra* Chapitre 8. La Loi sur la protection des données.

567 SCHOLZ, art. 4 ch. 4 RGPD, N 6 ; ARNING/ROTHKEGEL, art. 4 ch. 4 RGPD, N 112 ; HERBST/BUCHNER, art. 4 ch. 4 RGPD, N 6.

Enfin, une contradiction supplémentaire entre les travaux du Groupe de travail « Article 29 » et le RGPD doit être soulevée. En vertu des Lignes directrices, il existerait trois formes de profilage : un profilage « général », une prise de décision fondée sur un profilage et une prise de décision *exclusivement* automatisée, y compris le profilage[568]. Or, le RGPD ne prévoit aucun régime encadrant les décisions qui ne sont *pas* exclusivement automatisées. HÄUSELMANN souligne à juste titre que le RGPD fixe un cadre légal pour deux (et non trois) formes de profilage : un profilage qui peut conduire à une prise de décision qui n'est pas exclusivement automatisée et un profilage qui aboutit à une prise de décision exclusivement automatisée[569]. Le RGPD prévoit qu'un profilage (qui peut éventuellement être suivi d'une décision *non*-entièrement automatisée) doit être conforme aux principes généraux alors qu'un profilage qui serait suivi d'une décision individuelle automatisée doit également respecter les exigences de l'art. 22 RGPD[570]. Dans ce deuxième cas de figure, le profilage est considéré comme une sous-forme de la décision individuelle automatisée régie par l'art. 22 RGPD[571]. Ainsi, cette contradiction entre la prise de position du Groupe de travail « Article 29 » et la lettre du RGPD contribue à augmenter l'insécurité juridique en la matière. Aucune décision de justice, qui aurait pu clarifier ce point, n'a été rendue à ce jour.

Après avoir relevé les raisons pour lesquelles la rédaction de l'art. 4 ch. 4 RGPD est malencontreuse[572], il convient de se pencher sur les dispositions européennes, qui encadrent le traitement de données litigieux.

2. L'encadrement insuffisant du profilage en droit européen

L'art. 22 al. 1er RGPD, qui reprend en grande partie l'art. 15 DPD, fixe que « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ».

À titre préliminaire, on notera que la nature de cette disposition fait débat : est-ce que cette disposition interdit, par principe, la prise de décision automatisée, y compris le profilage, ou s'agirait-il « uniquement » de la consécration d'un droit de s'opposer à une décision individuelle automatisée ? À ce jour, la

568 Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 9.

569 HÄUSELMANN, N 5.

570 HÄUSELMANN, N 5.

571 ESSER, art. 4 ch. 4 RGPD, N 68 ; SCHREIBER, art. 4 ch. 4 RGPD, N 16 ; SCHWARTMANN/HERMANN, art. 4 ch. 4 RGPD, N 58.

572 SCHOLZ, art. 4 ch. 4 RGPD, N 1.

CJUE n'a pas tranché cette question. Si la doctrine est partagée quant à la réponse à cette question, une majorité estime que cette disposition consacre une interdiction de principe[573]. De surcroît, on retiendra que cette disposition porte expressément sur les décisions individuelles automatisées, qui peuvent se fonder sur un profilage effectué en amont à une telle décision. Ainsi, cette disposition cite l'utilisation d'un profilage en amont à une décision individuelle automatisée comme une utilisation possible (et fréquente) du profilage[574]. Cependant, cette disposition ne fixe aucun cadre matériel quant au profilage à lui seul. La licéité d'un profilage se déterminera dès lors sur la base des principes généraux fixés à l'art. 5 RGPD et les critères de licéité consacrés à l'art. 6 RGPD[575].

D'abord, on relèvera que la disposition ne s'applique uniquement aux « décisions (automatisées) ». Or, le RGPD ne précise pas ce qui doit être entendu par ce terme. En vertu de la doctrine, un profilage entendu comme l'« évaluation automatisée de certains aspects personnels » n'équivaut pas à une décision, mais constitue un des traitements de données qui peut précéder la décision (automatisée). En d'autres termes, si le profilage est un traitement de données qui génère de nouvelles connaissances, la décision automatisée est un acte créateur, qui déploie des effets définitifs à l'égard d'une personne individuelle[576].

En vertu de ce premier élément de cette disposition, la personne concernée a le droit ne pas « être soumise à une telle décision ». Une telle « soumission » à une « décision » doit être admise lorsque le responsable du traitement peut fixer unilatéralement les conditions de la décision individuelle automatisée[577].

---

573 HELFRICH, art. 22 RGPD, N 37 ss. ; dans le même sens et avec de nombreuses références supplémentaires, voir SCHOLZ, art. 22 RGPD, N 16 ; HÄUSELMANN quant à lui fait l'effort d'analyser les deux interprétations possibles afin d'arriver, à juste titre, à la conclusion que cette disposition consacre une interdiction de principe, voir, pour ces développements et de multiples références supplémentaires, HÄUSELMANN, N 18 ss. ; WACHTER, MITTELSTADT et FLORIDI se fondent sur les différentes implémentations de la DPD, qui contenait une disposition qui ressemblait à l'art. 22 RGPD (art. 15 DPD) . Certains États membres avaient consacré une interdiction, d'autres en revanche avaient prévu un droit d'opposition dans leur législation nationale. Sur la base de cette analyse, les auteurs estiment que les deux interprétations sont concevables. Dans le but de garantir un plus haut niveau de protection des droits des individus, ils plaident pour la consécration d'une interdiction de principe, voir WACHTER/MITTELSTADT/FLORIDI, pp. 94 s. et 98.

574 Pour une liste d'exemples très divers de tels profilages effectués en amont à une décision individuelle automatisée, voir SCHOLZ, art. 22 RGPD, N 22 ss.

575 À juste titre, SCHOLZ précise que seul le considérant 71, qui est non-contraignant, encourage les responsables de traitement à mettre en place des mesures techniques et organisationnelles appropriées lorsqu'ils effectuent un profilage (non-suivi d'une décision individuelle automatisée), voir SCHOLZ, art. 22 RGPD, N 20.

576 SCHOLZ, art. 22 RGPD, N 17.

577 SCHOLZ, art. 22 RGPD, N 18 ; dans le même sens, voir HELFRICH, art. 22 RGPD, N 43.

À titre d'exemple, on pensera à un profilage effectué dans le cadre d'une procédure d'embauche suivi d'une décision d'embaucher (ou pas) le candidat en question[578]. Au contraire, l'octroi automatisé d'un bonus dont les conditions auraient été fixées dans le contrat de travail ne constituerait pas une décision individuelle automatisée au sens de l'art. 22 al. 1er RGPD, mais plutôt un traitement de données automatisé qui vient confirmer une clause contractuelle[579].

Ensuite, la disposition a vocation à encadrer les traitements de données *entièrement* automatisés[580]. Un responsable du traitement ne saurait toutefois contourner cette disposition en prévoyant l'intervention factice d'une personne physique. Si une telle intervention humaine est prévue, la personne désignée doit jouir d'une réelle marge de manœuvre lui permettant d'influer sur la décision envisagée[581]. Une connaissance détaillée de l'algorithme ou du programme utilisé n'est en revanche pas nécessaire[582]. En d'autres termes, la simple confirmation de la décision proposée par le programme est sans influence sur le critère du « traitement exclusivement automatisé »[583]. Dans le contexte de l'emploi, SCHOLZ estime que la mise en place de classements automatisés sur la base de critères fixés en amont à la procédure d'embauche ou la présélection de candidats en fonction de certains paramètres comme p. ex. le sexe ou l'âge doivent être considérés comme des traitements de données, qui viennent faciliter la prise de décision (humaine), mais qui ne la remplacent pas. Dès lors, ces traitements de données ne tombent pas dans le champ de l'art. 22 RGPD. Au contraire, une notification automatique des candidats non-sélectionnés par un système d'*E-Recruiting* devrait être qualifiée de décision individuelle automatisée[584]. Au vu des exemples cités par SCHOLZ, on retiendra que de nombreux traitements de données partiellement, voire entièrement automatisés sur le lieu de travail ne sont pas encadrés par cette disposition et qu'à défaut de

578 SCHOLZ, art. 22 RGPD, N 24.

579 SCHOLZ, art. 22 RGPD, N 18 ; pour un avis contraire quant à la qualification d'un octroi automatisé d'un bonus, voir HÄUSELMANN, N 61. Cet exemple montre que la mise en pratique de ce critère peut s'avérer plus complexe que ce que pourrait laisser penser le texte légal.

580 On rappellera que si le profilage est également un traitement de données automatisé, l'évaluation envisagée grâce à un profilage ne doit pas être *entièrement* automatisée afin de tomber dans le champ de la définition du profilage telle que prévue à l'art. 4 ch. 4 RGPD. Ainsi, sur ce point, la définition du profilage est moins restrictive que celle qui fixe les contours de la décision individuelle automatisée.

581 HÄUSELMANN, N 37.

582 SCHOLZ, art. 22 RGPD, N 27.

583 HELFRICH, art. 22 RGPD, N 44 ; pour l'avis contraire, voir WACHTER/MITTELSTADT/FLORIDI, p. 92.

584 SCHOLZ, art. 22 RGPD, N 28.

précisions jurisprudentielles, la distinction entre une décision entièrement automatisée et un traitement de données automatisé, qui n'aboutit pas à une décision peut s'avérer délicate en pratique.

Enfin, une décision individuelle automatisée au sens du RGPD doit déployer des effets juridiques ou des effets significatifs sur la personne concernée. Une décision individuelle automatisée aura des effets juridiques si elle modifie le statut juridique de la personne concernée d'une manière ou d'une autre[585]. En droit privé, savoir si la non-conclusion d'un contrat modifie le statut des parties contractantes au sens du RGPD est controversée[586]. S'il est vrai que cette première hypothèse (effets juridiques) a suscité quelques réserves, la deuxième hypothèse (effets significatifs) a engendré de nombreuses critiques[587]. Une décision individuelle automatisée entraînant des conséquences négatives pour la personne concernée pourrait être qualifiée comme déployant de tels effets. En d'autres termes, la décision individuelle automatisée litigieuse doit avoir un impact non-négligeable sur la personne concernée ou influencer son comportement de manière significative. Il en irait ainsi d'un refus de conclure certains contrats[588] ou si la personne concernée se sent observée à la suite du traitement de données[589]. Les effets significatifs s'apprécieront toujours au cas par cas et d'un point de vue objectif[590]. Il découle de ces quelques développements qu'un profilage effectué lors d'une procédure d'embauche qui serait suivi d'un refus d'embauche automatisé pourra, dans de nombreux cas, être qualifié comme déployant des effets significatifs sur les candidats. Cette

585 HELFRICH, art. 22 RGPD, N 48.

586 HELFRICH estime que la non-conclusion d'un contrat modifie le statut juridique de la personne concernée, voir HELFRICH, art. 22 RGPD, N 48 ; SCHOLZ quant à lui est d'avis que le refus de conclure un contrat ne modifie *pas* le statut juridique de la personne concernée par le refus. Il admet toutefois une exception à cette lecture restrictive en précisant qu'un refus pourrait modifier le statut de la personne concernée si le responsable du traitement a porté atteinte à l'interdiction de discrimination, voir SCHOLZ, art. 22 RGPD, N 34 ; WACHTER, MITTELSTADT et FLORIDI estiment que la décision de ne pas embaucher un candidat ne modifie pas son statut juridique. Contrairement à SCHOLZ, ils n'avancent aucune exception à cette lecture restrictive, voir WACHTER/MITTELSTADT/FLORIDI, p. 93 ; À mon sens, il ne ressort pas clairement de la lettre du considérant 71 si le rejet automatique d'une demande de crédit en ligne et les pratiques de recrutement en ligne sans aucune intervention humaine cités en guise d'exemples doivent être considérés comme des exemples de décisions entraînant des effets juridiques ou affectant les personnes de manière significative ; HÄUSELMANN quant à lui semble attribuer ces deux exemples à la première hypothèse, voir HÄUSELMANN, N 39.

587 Pour un résumé de ces critiques, voir HÄUSELMANN, N 43 ss.

588 SCHOLZ, art. 22 RGPD, N 35 s.

589 HELFRICH, art. 22 RGPD, N 51.

590 SCHOLZ, art. 22 RGPD, N 35 ; HELFRICH, art. 22 RGPD, N 52.

qualification s'imposera d'autant plus si le secteur économique concerné a mis en place de telles procédures pour tous, voire presque tous les emplois dudit secteur. En bref, ce troisième élément de l'interdiction doit encore être précisé[591]. À ce stade, on notera qu'il est regrettable que le Législateur suisse ait repris ces trois imprécisions et ait, de surcroît, renoncé à consacrer une interdiction de principe dans la LPD révisée.

Quoiqu'il en soit, l'interdiction consacrée à l'art. 22 al. 1er LPD n'est pas absolue : les alinéas 2 à 4 de cette même disposition viennent définir des exceptions possibles à cette interdiction. Ainsi, un profilage effectué dans le contexte d'une procédure d'embauche qui serait suivi d'une décision individuelle automatisée peut être licite si la personne concernée y a explicitement consenti[592]. Or, le RGPD ne définit pas ce qui doit être entendu par « consentement explicite »[593]. Toutefois, tant cette question que celle de savoir quelles informations devront être mises à disposition de la personne concernée en amont à une telle décision ne jouent qu'un rôle marginal dans le cadre de la thématique définie. En effet, en raison du lien de subordination qui caractérise la relation de travail (y compris la procédure d'embauche), le consentement ne saurait être donné librement par le candidat[594].

De plus, les alinéas 2 à 4 prévoient que le profilage peut être licite s'il est prévu dans une loi d'un État membre, qui prévoit des mesures adéquates à la protection des droits des personnes concernées. Le considérant 71[595] fixe, à titre d'exemple, que les États membres pourraient prévoir, en droit national, de telles exceptions afin de lutter contre les fraudes et l'évasion fiscale ou d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement. Or, en plus d'être contraire au but d'harmonisation visé par la Commission, aucun État membre n'a fait recours à cette clause d'ouverture dans le

591 Dans le même sens, notamment à propos d'un refus d'embauche, voir WACHTER/MITTELSTADT/FLORIDI, p. 93.

592 On rappellera qu'en droit suisse, la LPD fixe que si un profilage à risque élevé entre particuliers se fonde sur le consentement de la personne concernée, ce consentement doit être exprès. Les notions de consentement explicite (droit européen) et consentement exprès (droit suisse) sont synonymes, voir dans le même sens, VASELLA, Einwilligung, N 33.

593 HÄUSELMANN, N 51 ; pour des précisions quant à cette question, voir Groupe de travail « Article 29 », Lignes directrices sur le consentement au sens du règlement 2016/679 du 28 novembre 2017, pp. 20 ss.

594 Dans le même sens, voir Groupe de travail « Article 29 », Lignes directrices sur le consentement au sens du règlement 2016/679 du 28 novembre 2017, pp. 7 s.

595 Pour un bref rappel de la valeur juridique de ces considérants en droit européen, voir WACHTER/MITTELSTADT/FLORIDI, p. 80.

contexte précis d'une procédure d'embauche[596]. Dès lors, tout comme la première exception prévue, cette deuxième exception n'a aucune portée dans le cadre de traitements automatisés effectués pendant la procédure d'embauche.

Enfin, une décision individuelle automatisée, qui se fonde sur un profilage peut exceptionnellement être licite si elle est considérée nécessaire à la conclusion d'un contrat. Dans le cadre de cette exception on peut alors de demander si le profilage du candidat puis la mise en place d'un programme permettant une prise de décision automatisée sont réellement nécessaires à la conclusion du contrat de travail. Il va sans dire qu'il incombe au responsable du traitement de déterminer si le traitement de données envisagé est nécessaire dans un cas d'espèce. Dès lors, force est de constater que si un employeur envisage de procéder à une décision individuelle automatisée, y compris un profilage, il estime qu'un tel traitement de données est nécessaire à la conclusion du contrat de travail[597]. Au vu des risques liés à l'utilisation du profilage dans le cadre d'une procédure d'embauche et des bénéfices encore peu déterminés de ce traitement suivi d'une décision individuelle automatisée, un employeur devrait faire preuve d'une certaine retenue dans l'appréciation du critère de nécessité[598]. Ceci est d'autant plus vrai que cette disposition introduit une insécurité juridique supplémentaire puisqu'elle fait peser la totalité de l'évaluation du critère de nécessité du traitement de données sur le responsable du traitement[599], c'est-à-dire sur l'employeur.

En son alinéa 3, l'art. 22 RGPD fixe que lorsqu'une décision individuelle automatisée, y compris un profilage, est considéré nécessaire à la conclusion du contrat de travail, il incombe au responsable du traitement de mettre en œuvre

596 On rappellera que dans le cadre précis du droit du travail, les États membres ne peuvent pas consacrer, en droit national, un régime moins protecteur que le régime général consacré par le RGPD, notamment en raison de l'art. 88 RGPD, qui couvre également les traitements de données effectués pendant la procédure d'embauche, voir, pour plus de précisions quant à la portée de l'unique disposition du RGPD qui porte spécifiquement sur la protection des droits des employés, DAEDELOW, p. 35 ; pour des exemples de mise en œuvre de cette clause d'ouverture en droit allemand, qui ne concernent pas le droit du travail, voir SCHOLZ, art. 22 RGPD, N 48 ss.

597 HÄUSELMANN, N 49 ; à juste titre, WACHTER, MITTELSTADT et FLORIDI précisent que cette exception a pour conséquence que si le responsable du traitement décide que le traitement automatisé est nécessaire à la conclusion du contrat, le consentement de la personne concernée par ce traitement ne doit pas être recherché. En d'autres termes, la personne concernée ne peut pas s'opposer en amont au traitement de données en refusant de donner son consentement. La personne concernée ne dispose alors que des droits découlant de l'art. 22 al. 3 RGPD, voir WACHTER/MITTELSTADT/FLORIDI, p. 94.

598 Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, pp. 14 et 26.

599 HÄUSELMANN, N 49.

les mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. La personne concernée a alors, à tout le moins, le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision. Dans le cadre de l'analyse de ce troisième alinéa, trois aspects méritent d'être relevés.

D'abord, on notera que savoir si cette disposition comprend non seulement le droit à une intervention humaine et le droit de faire valoir son point de vue, mais aussi un véritable droit à l'explication laisse la doctrine partagée[600]. Si une interprétation généreuse de cette disposition est retenue, un candidat qui n'aurait pas été retenu pour une place de travail sur la base d'une évaluation automatisée négative pourrait demander l'intervention de l'employeur ou d'un membre des ressources humaines. Cette personne ne devra pas lui expliquer le programme utilisé en détails, mais devra préciser quels aspects ont été déterminants lors du refus. La personne candidate devra être en mesure de vérifier si des données erronées ont été traitées ou si les spécificités du contexte n'ont pas été considérées à leur juste mesure[601]. On notera toutefois que même si cette interprétation large du droit à l'explication est retenue, une explication compréhensible d'un programme, qui se caractérise par son opacité, implique, très souvent, que le responsable du traitement procède à une réduction des paramètres qui ont été pris en compte dans la décision. Cette sélection des paramètres qui vont être dévoilés à la personne concernée peut alors s'avérer arbitraire[602].

Ensuite, ce droit doit s'exercer vis-à-vis d'une personne qui a l'autorité de modifier la décision. Cette personne devra alors procéder à une analyse tant des données traitées automatiquement que des données supplémentaires éventuellement soumises par la personne concernée. Or, en raison de la liberté contractuelle, cette disposition ne fixe en aucun cas une obligation, pour le responsable du traitement, de modifier la décision. Indépendamment de la lecture privilégiée, il est douteux que cette intervention humaine entraîne, pour les personnes concernées, des avantages considérables en pratique[603].

Enfin, on notera que le droit de contester la décision permet au candidat de faire valoir son désaccord avec la décision individuelle automatisée à laquelle

600 HÄUSELMANN ainsi que WACHTER, MITTELSTADT et FLORIDI estiment que le RGPD ne consacre pas un tel droit à l'explication, voir HÄUSELMANN, N 53 et WACHTER/MITTELSTADT/FLORIDI, pp. 79 ss. Ces derniers précisent toutefois que la consécration d'un tel droit n'est pas exclue dans le futur. Ils fondent leur analyse sur le considérant 71 (non-contraignant) et les travaux législatifs du RGPD ; SCHOLZ, au contraire, est d'avis qu'un tel droit découle de cette disposition, voir SCHOLZ, art. 22 RGPD, N 57 ; HELFRICH quant à lui ne prend pas clairement position, voir HELFRICH, art. 22 RGPD, N 69 ss.

601 SCHOLZ, art. 22 RGPD, N 57.

602 AlgorithmWatch, p. 33.

603 HÄUSELMANN, N 53.

il a été soumis. Or, il ne s'agit pas d'un droit d'opposition tel que prévu à l'art. 21 RGPD. En d'autres termes, l'exercice de ce droit ne rend pas automatiquement illicite la décision individuelle automatisée. Savoir si cette disposition confère une voie de droit supplémentaire est controversé[604].

S'il est vrai que l'art. 22 RGPD constitue la disposition phare parmi les nouvelles dispositions, qui encadrent les décisions individuelles automatisées, y compris le profilage, d'autres dispositions du RGPD fixent également des obligations incombant aux responsables du traitement. En sus des principes généraux consacrés à l'art. 5 RGPD et des conditions de licéité fixées à l'art. 6 RGPD[605], on pensera, d'une part, aux art. 13 al. 2 let. f et 14 al. 2 let. g RGPD qui prévoient que le responsable du traitement doit informer les personnes concernées de « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'art. 22 al. 1er et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». L'art. 12 al. 1er RGPD précise que ces informations doivent être transmises à la personne concernée « d'une façon concise, transparente, compréhensible et aisément accessible »[606]. En aucun cas, la complexité éventuelle du traitement de données ne saurait justifier une quelconque violation de cette obligation[607].

On notera que pris à la lettre, les art. 13 al. 2 let. f et 14 al. 2 let. g RGPD impliquent que l'obligation d'informer la personne concernée ne doit être respectée uniquement lorsque le responsable du traitement envisage une décision individuelle automatisée, qui se fonde, p. ex. sur un profilage. Or, si une telle lecture est fidèle au texte légal, elle est contraire au considérant 60 qui prévoit que « la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci ». Dans ses lignes directrices, le Groupe de travail « Article 29 » semble privilégier cette deuxième lecture plus proche de la lettre du considérant (non-contraignant)[608]. Appliquée au cas d'espèce, une telle lecture téléologique de ces deux dispositions du RGPD impliquerait que l'employeur européen doit honorer cette obligation même lorsqu'il procède à

604 Pour un avis contre la consécration d'une voie de droit supplémentaire, voir SCHOLZ, art. 22 RGPD, N 61 ; pour un avis en faveur d'une telle consécration (avant tout lors d'un traitement effectué par une autorité publique), voir HELFRICH, art. 22 RGPD, N 72.

605 Pour une comparaison extensive entre les dispositions du RGPD et le projet de LPD (qui n'a plus subi de modifications majeures à la suite de la publication de cette contribution), voir FÜZESSÉRY/SCHNEIDER, pp. 144 ss.

606 On rappellera que ces diverses dispositions viennent préciser le principe de transparence tel que consacré à l'art. 5 RGPD, voir DAEDELOW, p. 35.

607 SCHOLZ, art. 22 RGPD, N 58.

608 Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, p. 18.

un profilage qui n'est pas suivi d'une décision individuelle automatisée. En plus de cette première incertitude qui entoure ces deux dispositions, HÄUSELMANN relève, à juste titre, que le contenu de cette information devra encore être précisé[609].

D'autre part, l'art. 15 al. 1er let. h RGPD prévoit un droit d'accès en aval dont la portée correspond à celle (incertaine) des art. 13 et 14 RGPD. Les contours exacts de ce droit devront encore faire l'objet de précisions[610]. À ce stade, on notera que les exceptions au droit d'accès que pourrait faire valoir l'employeur devront être admises avec retenue[611] et que le sous-traitant, comme p. ex. le courtier en données, peut être tenu de soutenir le responsable du traitement dans sa démarche[612].

Enfin, dans une veine plus technique, on rappellera que l'art. 35 al. 3 let. a RGPD oblige le responsable du traitement à procéder à une analyse d'impact lorsqu'il envisage une prise de décision automatisée qui serait fondée sur un profilage. Le non-respect de cette obligation peut entraîner de lourdes amendes administratives[613]. Une violation des autres obligations analysées plus haut (art. 12-15 et 22 RGPD) peut entraîner des amendes administratives encore plus importantes[614].

3. Conclusion intermédiaire

Même s'il est vrai que l'UE peut se féliciter d'avoir été l'organisation internationale à avoir adopté les premières dispositions contraignantes encadrant le profilage, qui sont directement applicables entre particuliers, quelques problématiques ont pu être relevées dans le cadre de la brève analyse du cadre légal européen. Plusieurs insécurités juridiques subsistent avant tout par rapport aux contours exacts des notions suivantes : D'une part, il n'est pas toujours aisé de savoir ce qui doit être entendu par « évaluation de certains aspects personnels »

609 HÄUSELMANN, N 56 s. ; dans une veine similaire, avec de plus amples développements, voir WACHTER/MITTELSTADT/FLORIDI, pp. 82 s.

610 Pour une analyse approfondie du droit d'accès tel que mis en œuvre par les États membres sous le régime de la DPD, l'impact de ces dispositifs nationaux sur l'interprétation du droit d'accès désormais consacré par le RGPD et la question controversée de savoir quelles informations devraient être mises à disposition des personnes concernées, voir WACHTER/MITTELSTADT/FLORIDI, pp. 83 ss. et 97.

611 À titre d'exemple, on consultera la publication de GRIESINGER, qui offre un résumé des aspects principaux quant à la mise en œuvre de l'art. 15 RGPD et une analyse de deux arrêts, portant sur cette disposition, rendus par des tribunaux allemands. L'un d'entre eux concernait précisément un rapport de travail, voir GRIESINGER, N 20 ss.

612 Art. 28 al. 3 let. e RGPD.

613 Art. 83 al. 4 let. a RGPD.

614 Art. 83 al. 5 let. b RGPD.

en vertu de l'art. 4 ch. 4 RGPD. D'autre part, tant la notion de « décision exclusivement automatisée » que celle d'« effets significatifs », mentionnées à l'art. 22 al. 1er RGPD, devront faire l'objet de précisions. Il en va de même de la notion de « consentement explicite » et du critère de « nécessité d'une décision individuelle automatisée à la conclusion d'un contrat », qui sont cités parmi les exceptions à l'interdiction des décisions individuelles automatisées.

Ensuite, plusieurs contradictions entre les publications du Groupe de travail « Article 29 » et la lettre des dispositions commentées ont pu être mises en lumière. On pensera notamment à la contradiction entre les Lignes directrices, qui précisent que les deux premières étapes d'un profilage peuvent porter sur des données anonymes, et la définition consacrée par le RGPD qui n'englobe uniquement les traitements de données à caractère personnel. De surcroît, l'analyse ci-dessus a révélé une incertitude quant au contenu exact de l'obligation d'informer la personne concernée soumise au profilage. En présence d'un profilage qui ne serait pas suivi d'une décision individuelle automatisée, il n'est pas clair si le responsable du traitement doit également informer la personne concernée quant à la logique sous-jacente ou si cette information ne doit être procurée à la personne concernée uniquement si le profilage est suivi d'une décision individuelle automatisée.

Enfin, les mesures mises à disposition des personnes concernées restent floues et ne semblent que peu efficaces en pratique : la consécration du droit de demander une intervention humaine répond certes à la crainte d'être soumis à une décision prise par une machine, mais, dans sa forme actuelle, ne semble pas constituer une réponse adéquate aux défis engendrés par le profilage dans le cadre d'une procédure d'embauche.

Il découle de ce qui précède qu'un profilage effectué dans le cadre d'une procédure d'embauche n'est qu'incomplètement encadré par le RGPD[615]. Ainsi, ce dispositif peut certes servir de source d'inspiration, mais ne constitue pas un modèle juridique à suivre dans sa totalité. Le Parlement suisse a repris la définition du profilage et, en grande partie, le régime européen qui encadre ce nouveau traitement de données. En effet, comme nous avons pu le constater plus haut, le Parlement suisse s'est contenté de définir le profilage sans pour autant prévoir un régime spécifique pour ce traitement de données. Dès lors, il est regrettable, d'une part, que le Parlement suisse n'ait pas su « profiter » des erreurs du Législateur européen quant à la définition à donner au profilage et, d'autre part, qu'il ait décidé de ne pas prévoir un régime renforcé pour le profilage qui peut pourtant avoir des répercussions importantes sur les droits des citoyens suisses. Ainsi, il convient de se pencher sur d'autres dispositifs

615 Dans le même sens, voir AlgorithmWatch, pp. 45 ss.

fédéraux qui pourraient éventuellement contribuer à encadrer le profilage lors d'une procédure d'embauche, notamment la Loi sur l'égalité entre femmes et hommes, la Loi sur l'élimination des inégalités frappant les personnes handicapées, la Loi sur l'analyse génétique humaine, la Loi sur le travail et l'artisanat ou encore le Code pénal.

Chapitre 9. Autres dispositifs fédéraux potentiellement applicables

S'agissant de répondre à de nouvelles questions qui se posent dans le cadre de la relation de travail, un examen plus approfondi de la LEg (A) et de la LHand (B) s'avère nécessaire. Il en va de même des dispositions potentiellement pertinentes de la LAGH (C) et de la LTr (D) ainsi que du régime pénal (E). Ce chapitre se terminera par un bref résumé de l'analyse de ces différentes dispositions potentiellement applicables à un profilage effectué dans le cadre d'une procédure d'embauche (F).

A. La Loi fédérale sur l'égalité entre femmes et hommes

La Loi fédérale sur l'égalité entre femmes et hommes[616] (ci-après « LEg ») a pour but de promouvoir dans les faits l'égalité entre femmes et hommes[617]. Ainsi, cette loi contribue à concrétiser l'art. 8 al. 3 Cst., qui consacre l'égalité entre femmes et hommes et, sur le plan privé, vient préciser un aspect du devoir d'assistance de l'employeur tel que fixé à l'art. 328 CO[618]. La LEg est entrée en vigueur le 1er juillet 1996 et a ponctuellement été révisée depuis[619]. Elle s'applique aux rapports de travail régis soit par le CO soit par le droit public fédéral, cantonal ou communal[620]. L'interdiction de toute discrimination vaut pour

616 Loi fédérale sur l'égalité entre femmes et hommes (LEg) du 24 mars 1995, RS 151.1.

617 Art. 1er LEg.

618 Voir *supra* Chapitre 7. Le Code des obligations.

619 La révision la plus importante est entrée en vigueur le 1er juillet 2020. À partir de cette date, les employeurs qui occupent au moins 100 personnes sont tenus d'effectuer une analyse de l'égalité salariale dans un délai d'un an, de la faire contrôler par un organe indépendant et d'informer leurs collaboratrices et collaborateurs, ainsi que les actionnaires, des résultats (art. 13*a* à 13*i* LEg) ; pour un aperçu des différentes analyses effectuées par divers organes indépendants en 2021, voir STECK, Frauen werden kaum diskriminiert, wie die neue Überprüfung der Löhne zeigt.

620 Art. 2 LEg.

tous les domaines de la vie professionnelle, c'est-à-dire également pour la phase précontractuelle de l'embauche[621]. Cette interdiction est absolument impérative, la faute ne jouant aucun rôle[622].

L'art. 8 LEg vient préciser la procédure à suivre en cas de discrimination à l'embauche. Cette disposition prévoit, d'une part, que le candidat qui n'est pas engagé et qui se prévaut d'une discrimination peut exiger de l'employeur qu'il motive sa décision par écrit. D'autre part, le deuxième alinéa fixe que si la personne concernée souhaite faire valoir son droit à une indemnité, elle dispose d'un délai de trois mois à compter du moment où le refus d'embauche lui a été communiqué, sous peine de péremption. Dans ce contexte, trois éléments méritent d'être analysés plus en détail.

D'abord, le premier alinéa de cette disposition prévoit que le candidat non-embauché est en droit de demander une explication par écrit quant aux raisons qui ont conduit au refus de l'employeur[623]. Toutefois, il va sans dire qu'en pratique, l'employeur sera tenté d'avancer une raison qui n'est pas liée au sexe du candidat afin de justifier son refus de l'embaucher. Dès lors, il n'est pas certain que cette disposition parvienne en effet à faciliter la preuve d'un refus d'embauche discriminatoire[624]. Même dans l'hypothèse où l'employeur répondait qu'il a effectué un profilage et qu'il soupçonne que cette évaluation automatisée a eu un effet discriminatoire sur la personne concernée, la LEg ne prévoit aucune précision quant au contenu d'une telle explication. À ce sujet, RIEMER-KAFKA et UEBERSCHLAG précisent qu'en vertu de la *ratio legis*, les explications quant au refus d'embauche doivent être complètes et aussi détaillées que nécessaire à la détermination de la raison du refus[625]. Les démarches statistiques qui sous-tendent le profilage sont, la plupart du temps, incompréhensibles pour une personne qui n'est pas spécialisée dans ce domaine. En d'autres termes, il n'est pas certain que ce droit à l'information consacré au premier alinéa soit très efficace dans un monde du travail de plus en plus numérisé.

On notera au surplus, qu'en fonction des bases de données dépouillées, les évaluations automatisées subséquentes pourraient se révéler discriminatoires

621 Art. 3 al. 2 LEg.

622 WYLER/HEINZER, p. 79 avec des références supplémentaires.

623 Ainsi, la LEg ne prévoit aucune obligation de demander une telle explication. En d'autres termes, la personne concernée peut engager une action en justice sans avoir fait valoir son droit à une explication tel que consacré à l'art. 8 al. 1er LEg, voir, à titre d'exemple, UEBERSCHLAG, p. 122 ; cette disposition ressemble aux art. 335 al. 2 et 337 al. 1er CO. La jurisprudence et la doctrine relatives à ces deux dispositions du CO peuvent être appliquées par analogie dans le contexte de cette contribution, voir RIEMER-KAFKA/UEBERSCHLAG, art. 8 al. 1er LEg, N 11 ou BIGLER-EGGENBERGER, art. 8 LEg, N 11.

624 RIEMER-KAFKA/UEBERSCHLAG, art. 8 al. 1er LEg, N 26.

625 RIEMER-KAFKA/UEBERSCHLAG, art. 8 al. 1er LEg, N 15.

au sens de la LEg. À cet égard, LEMPEN rappelle, à juste titre, que « les données qui se trouvent sur Internet ne sont pas nécessairement correctes et s'avèrent souvent incomplètes ou stéréotypées. Sur l'encyclopédie Wikipédia, par exemple, les articles au sujet de femmes célèbres sont plus rares et mettent davantage l'accent sur les aspects de leur vie privée que sur leur apport intellectuel. De façon générale, les femmes apparaissent dans les médias beaucoup moins souvent que les hommes et sont rarement présentées comme des expertes sur le plan professionnel. Dès lors, une décision d'embauche fondée sur la façon dont les personnes candidates sont présentées sur Internet peut s'avérer discriminatoire au sens de l'art. 3 LEg »[626].

En bref, reste à savoir ce qui doit être entendu par « explications complètes et aussi détaillées que nécessaire » lorsqu'il s'agit de déterminer si un profilage a été discriminatoire ou pas. Face aux difficultés de comprendre le raisonnement sous-jacent au profilage on peut se demander s'il ne serait pas judicieux d'étendre l'allégement du fardeau de la preuve tel que prévu à l'art. 6 LEg aux procédures d'embauche[627].

Ensuite, il convient de noter que la LEg ne s'applique uniquement qu'en cas de refus d'embauche. En d'autres termes, un candidat qui a été embauché sur la base d'un profilage favorable, mais qui se sent tout de même mal à l'aise à la suite de la mise en place de cette mesure de surveillance, ne pourra pas agir contre l'employeur sur la base de la LEg[628]. Ainsi, la LEg ne semble pas être un instrument efficace pour encadrer les mesures de surveillance dans le cadre de procédures de recrutement *de manière générale*.

Enfin, on notera que le Législateur ne souhaitait pas limiter la liberté contractuelle de manière excessive[629]. Ainsi, même en cas de profilage discriminatoire, la personne concernée n'aura pas le droit de se faire engager, p. ex. sur la base d'une procédure « à l'ancienne », mais ne pourra que faire valoir son droit à une indemnité. Cette indemnité sera fixée compte tenu de toutes les circonstances et calculée sur la base du salaire auquel la personne discriminée

626 LEMPEN, p. 284.

627 Dans le même sens, mais proposant un allégement du fardeau de la preuve dans le cadre de *toutes* les procédures d'embauche, c'est-à-dire pas seulement dans le cadre de procédures d'embauche basées sur un profilage potentiellement discriminatoire en raison du sexe, voir UEBERSCHLAG, p. 126.

628 Il va sans dire qu'en pratique, notamment au vu des enjeux économiques et du lien de subordination qui caractérisent les relations de travail, il n'est que peu probable qu'un employé fraîchement embauché engage une action en justice dans les trois mois après avoir commencé son nouvel emploi ; il en va autrement du régime prévu par le CO et la LPD respectivement, voir *supra* Chapitre 7. Le Code des obligations et Chapitre 8. La Loi sur la protection des données.

629 FF 1993 1237.

aurait vraisemblablement eu droit[630]. En tous les cas, le montant n'excédera pas le montant correspondant à trois mois de salaire[631]. Si malgré tous les obstacles décrits ci-dessus, la personne concernée parvient à prouver un refus d'embauche discriminatoire et ainsi à faire valoir son droit à une indemnité, force est de constater que l'indemnité qui pourra être touchée reste relativement basse. Dès lors, on peut douter que le régime mis en place par la LEg ait un effet dissuasif[632].

Dans une veine plus générale, il convient de relever que la LEg n'encadre que les éventuelles discriminations entre femmes et hommes dans les rapports de travail. Les autres formes de discrimination entendues comme une forme d'atteinte à la personnalité[633] ne sont pas couvertes par cette loi. En d'autres termes, le champ d'application de la LEg est restreint au vu des nombreuses discriminations possibles dans le cadre d'une procédure d'embauche, notamment à la suite d'un profilage. En effet, comme nous l'avons vu au chapitre préliminaire, la quantité de données traitées dans le cadre d'un profilage est considérable.

Il découle de ces quelques observations que la portée de la LEg dans le cadre d'un profilage effectué lors d'une procédure de recrutement semble limitée.

Dans le domaine du travail, le principe de non-discrimination n'est non seulement concrétisé par la LEg, mais aussi par la Loi du 13 décembre 2002 sur l'égalité pour les handicapés[634] (ci-après « LHand »). Dès lors, il convient de se pencher sur cette loi fédérale entrée en vigueur le 1er janvier 2004 afin de déterminer si elle contient une ou plusieurs disposition(s) qui viendrai(en)t encadrer le profilage dans le cadre d'une procédure d'embauche.

B. La Loi fédérale sur l'égalité pour les handicapés

L'art. 1er LHand fixe que la LHand « a pour but de prévenir, de réduire ou d'éliminer les inégalités qui frappent les personnes handicapées. [Cette loi] crée les conditions propres à faciliter aux personnes handicapées la participation à la vie en société, en les aidant notamment (...) dans l'exercice d'une activité professionnelle ». Malgré cette disposition qui semble être applicable à tous les rapports de travail, la LHand ne vise que les rapports de travail régis par la Loi

630 Art. 5 al. 2 et art. 8 LEg.

631 Art. 5 al. 4 LEg.

632 Dans le même sens, voir DUNAND, Discrimination à l'embauche, p. 69.

633 Art. 6 al. 1er et 30 al. 2 let. a LPD.

634 Loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (LHand) du 13 décembre 2002, RS 151.3.

sur le personnel de la Confédération[635], (ci-après « LPers »). Il découle de cette constatation ainsi que des développements ci-dessus relatifs à la LPD et au CO que l'employeur privé n'est pas tenu de faire preuve d'égards particuliers en faveur des personnes handicapées lors de l'embauche. Les personnes handicapées ne disposent donc d'aucune protection particulière à cet égard[636] bien que le Conseil fédéral ait reconnu que le fait de pouvoir accéder au marché de l'emploi et y être apprécié pour ses qualifications est d'une importance capitale pour l'individu, économiquement et socialement[637]. Dès lors, une personne candidate dont un handicap dépourvu d'un lien quelconque avec son aptitude au travail serait révélé par un profilage effectué par l'employeur privé ne pourra contester ce profilage uniquement sur la base des dispositions générales du CO et de la LPD. Ainsi, la LHand n'offre aucun encadrement supplémentaire du profilage dans le cadre d'une procédure de recrutement de droit privé.

C. La Loi fédérale sur l'analyse génétique humaine

Les développements technologiques récents ont profondément modifié la qualité des analyses génétiques et le réseau des laboratoires. Par ailleurs, de nouvelles découvertes sur les liens entre les gènes et les caractéristiques humaines ont bouleversé la compréhension des possibilités et de la pertinence des analyses génétiques[638]. La complexité de ces nouvelles technologies et la possibilité d'obtenir, en une seule analyse, de nombreux résultats sur le patrimoine génétique, même sans les avoir recherchés, soulèvent de nombreuses nouvelles questions, notamment concernant l'information et le conseil, le consentement, le droit à ne pas être informé, la conservation et la réutilisation des échantillons et des données génétiques[639]. Dans le contexte de la présente contribution, il convient avant tout de mentionner les analyses concernant le mode de vie. Cette nouvelle forme d'analyses génétiques permet de déterminer de mieux en mieux des caractéristiques qui ne fournissent aucune information sur les prédispositions pathologiques ou les risques de santé de la personne

635 Loi sur le personnel de la Confédération (LPers) du 24 mars 2000, RS 172.220.1 ; cela étant, la LHand déploie quelques effets entre particuliers. En effet, cette loi oblige les particuliers eux-mêmes pour diverses constructions et installations, voir l'art. 3 LHand et, pour une brève analyse critique de la définition jugée trop étroite de la notion de « discrimination » telle qu'entendue par la LHand et l'Ordonnance y relative, voir MARTENET, La protection, pp. 424 s.

636 WYLER/HEINZER, p. 84.

637 FF 2001 1616.

638 FF 2017 5261 ; dans le même sens, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 44.

639 FF 2017 5262.

concernée. À titre d'exemple, il s'agit d'analyses relatives aux compétences sportives et à l'alimentation ou qui portent sur l'apparence, à l'instar de la couleur des cheveux ou des yeux[640]. Cette évolution a impliqué une ré-évaluation de certains éléments fondamentaux de la Loi fédérale sur l'analyse génétique humaine[641] (ci-après « aLAGH ») entrée en vigueur le 1er juillet 2007. Ainsi, le régime encadrant les analyses génétiques dans le domaine des rapports de travail a été révisé. L'entrée en vigueur de ce régime précisé est prévue pour le 1er décembre 2022. Dans ce contexte, on notera que le Comité des Ministres du Conseil de l'Europe a également constaté que l'utilisation de nouvelles méthodes de traitements de données par les employeurs pouvait présenter des risques pour les droits et libertés fondamentales des employés. Ainsi, il a adopté la Recommandation CM/Rec(2015)5 sur le traitement des données à caractère personnel dans le cadre de l'emploi (ci-après « Recommandation emploi ») le 1er avril 2015 qui, en ses art. 9.2 ss., propose un cadre pour les traitements de données génétiques effectués dans le cadre de procédures de recrutement.

Il va sans dire que toute analyse de données génétiques d'une personne se portant candidate à un poste donné constitue un traitement de données sensibles au sens de la LPD[642]. Si cette analyse se fait de manière entièrement automatisée, il s'agit d'un profilage au sens de la LPD (voire d'un profilage à risque élevé)[643]. Dès lors, une telle analyse effectuée dans le cadre d'une procédure de recrutement devra non seulement être conforme à la LAGH, mais aussi aux dispositions de la LPD (et du CO). Ainsi, il convient de se pencher sur le régime révisé avec un accent tout particulier sur la protection des données.

L'art. 37 LAGH fixe une interdiction de principe selon laquelle l'employeur ne peut ni exiger la réalisation d'analyses génétiques en dehors du domaine médical, ni demander ou utiliser des données génétiques non pertinentes du point de vue médical. À cet égard, le Message précise, à mon sens à juste titre, qu'« aucun argument ne plaide pour une utilisation de données génétiques ne relevant pas du domaine médical dans le cadre de rapports de travail »[644]. Il découle de cette interdiction que l'employeur ne saurait procéder à une analyse concernant le mode de vie du candidat[645]. De plus, dans l'hypothèse où le candidat aurait déjà effectué une analyse concernant son mode de vie dans un

640 FF 2017 5263.

641 Loi fédérale sur l'analyse génétique humaine du 8 octobre 2004 (LAGH), RS 810.12.

642 Dans le même sens, voir l'art. 9.1 Recommandation emploi.

643 Notons que la Recommandation emploi ne propose aucune définition du profilage, voire du profilage à risque élevé.

644 FF 2017 5358.

645 Dans le même sens, voir l'art. 9.3 Recommandation emploi.

contexte antérieur à la procédure d'embauche et qu'il déciderait de la mettre à disposition de l'employeur, l'employeur n'est pas en droit de l'utiliser dans le cadre de la procédure de recrutement (car en dehors du domaine médical)[646].

Il ne s'agit toutefois pas d'une interdiction absolue. En effet, l'art. 38 al. 1er LAGH prévoit que les analyses génétiques (médicales)[647] prescrites en lien avec des rapports de travail peuvent être réalisées dans le but de déterminer les caractéristiques ayant un rapport avec le poste concerné. Cette disposition se fait l'écho de l'art. 328b CO qui fixe que l'employeur peut procéder à tout traitement de données personnelles portant sur les aptitudes du travailleur à remplir son emploi. Ainsi, l'employeur peut accéder aux données génétiques du candidat si elles portent sur l'aptitude à remplir l'emploi[648]. Si l'employeur procède à une analyse génétique diagnostique, il suffira de respecter les exigences fixées à l'art. 38 LAGH. Si toutefois il compte procéder à une analyse génétique présymptomatique, il faudra également tenir compte du régime fixé aux art. 39 et 40 LAGH[649].

L'art. 38 al. 2 LAGH quant à lui prévoit que le médecin communique le résultat de l'analyse uniquement au candidat. Le médecin peut uniquement indiquer à l'employeur si la personne concernée entre ou n'entre pas en considération pour l'activité envisagée[650]. Cette disposition reflète le principe de proportionnalité tel que consacré à l'art. 6 al. 2 LPD dans la mesure où ce principe prévoit, entre autres, que les données doivent être transmises uniquement aux personnes qui nécessitent ces données afin d'accomplir leurs fonctions. L'employeur ne doit, en effet, seulement savoir si le candidat est apte à pourvoir le poste ou pas. Pour ce faire, il ne doit pas avoir accès à un éventuel diagnostic médical.

---

646 En pratique, on peut bien évidemment se demander à quel point cette interdiction d'utiliser des analyses génétiques effectuées antérieurement à la procédure d'embauche peut être mise en œuvre. En effet, si un candidat, p. ex. parce qu'il ignore le cadre légal pertinent, met une telle analyse à la disposition de l'employeur, il n'est pas exclu qu'une telle information supplémentaire influence le choix de l'employeur (dans un sens ou dans un autre) ; dans le même sens à propos de l'interdiction de l'utilisation d'analyses génétiques présymptomatiques, voir MUND, p. 251.

647 Art. 37 LAGH *a contrario*.

648 FF 2017 5359.

649 En effet, désormais, l'art. 38 LAGH est formulé de sorte à s'appliquer aux analyses génétiques tant diagnostiques que présymptomatiques, voir, pour de plus amples développements à ce sujet, FF 2017 5360 ; un encadrement plus strict des analyses génétiques présymptomatiques semble justifié dans la mesure où ce sont ces analyses qui constituent le plus grand risque d'atteinte aux droits fondamentaux, voir MUND, pp. 253 s. ; dans le même sens, mais en de termes légèrement différents, voir l'art. 9.3 Recommandation emploi.

650 Dans le même sens, voir l'art. 9.5 Recommandation emploi.

Si les interdictions consacrées aux art. 37 LAGH (interdiction d'analyses génétiques non-médicales) et 38 al. 1er LAGH (interdiction d'analyses génétiques médicales dépourvues de lien avec les rapports de travail) sont absolues, il en va autrement de celle fixée à l'art. 39 LAGH (interdiction d'analyses génétiques médicales présymptomatiques). En effet, l'art. 40 LAGH prévoit une exception à cette dernière interdiction : à condition que l'employeur respecte toutes les conditions qui sont fixées dans cette disposition, il peut effectuer des analyses génétiques présymptomatiques d'un candidat.

Enfin, l'art. 41 LAGH soumet ces analyses génétiques à la surveillance des inspecteurs cantonaux tels qu'institués par la Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce[651] (ci-après « LTr »). Cette disposition, qui vient ancrer ce régime dans le droit du travail public, a pour conséquence que tout candidat qui s'estime lésé par une analyse génétique automatisée peut s'adresser à l'inspecteur compétent et ne doit donc pas attaquer l'employeur en justice. Comme nous l'avons déjà vu plus haut, il est peu probable que le candidat porte plainte contre l'employeur devant un juge civil. En tant que candidat, voire en tant qu'employé, il est souvent plus commode de s'adresser à une autorité de surveillance impartiale. Une telle règle a donc pour conséquence que les personnes concernées peuvent mieux faire respecter leurs droits[652].

Il découle de cette brève présentation du cadre légal prévu par l'aLAGH (puis légèrement révisé), que le Législateur a été clairvoyant, notamment en anticipant la réalisation d'analyses génétiques ou l'utilisation des résultats d'analyses antérieures aux rapports de travail. L'importance pratique de ce cadre légal semble (encore) limitée, mais cela risque de changer[653]. Il n'en demeure pas moins que le Législateur a su trouver un équilibre entre les intérêts de l'employeur (divers intérêts avant tout d'ordre économique)[654] et de l'employé (protection adéquate de sa santé sur le lieu de travail, prévention d'atteintes aux droits de tiers, protection de sa personnalité)[655] en prévoyant une

651 Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce (Loi sur le travail, LTr) du 13 mars 1964, RS 822.11.

652 Il convient de noter que la LAGH révisée ne change rien aux compétences des autorités en termes d'exécution de la LAGH, voir FF 2017 5256.

653 FF 2017 5359.

654 Dans le cadre d'analyses génétiques présymptomatiques toutefois, il semblerait que l'employeur ne puisse invoquer ses intérêts économiques afin de justifier un tel traitement de données. En effet, au regard de l'art. 40 al. 1er let. a LAGH, il semble que seul l'intérêt prépondérant du candidat à voir sa santé protégée, voire un intérêt public prépondérant, comme p. ex. la protection de l'environnement ou les droits de tiers, peuvent justifier une telle atteinte à la personnalité du candidat, voir dans le même sens, MUND, pp. 254 s.

655 Pour une analyse plus approfondie des divers intérêts potentiellement concernés dans ces constellations, voir MUND, pp. 188 ss.

interdiction de principe avec quelques exceptions strictement encadrées[656]. Ce faisant, il a également contribué à mettre en œuvre la Recommandation emploi du Comité des Ministres[657]. Ce régime nuancé, mais malheureusement limité aux traitements de données génétiques (automatisés ou pas) pendant la procédure d'embauche, pourrait néanmoins servir d'inspiration au Législateur, notamment s'il s'apprête à déterminer un encadrement plus efficace du profilage dans le cadre de procédures de recrutement. En d'autres termes, il serait à espérer qu'il encadre non seulement les traitements de données génétiques dans le cadre de procédures de recrutement, mais aussi, de manière plus générale, les traitements de données sensibles (automatisés) effectués lors d'une procédure d'embauche.

D. La Loi sur le travail et l'Ordonnance 3 y relative

Lorsque la Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce[658] (ci-après « LTr ») a été adoptée en 1964, cette loi répondait à deux besoins. D'une part, il s'agissait d'étendre le champ d'application de la législation fédérale sur la protection des travailleurs à l'ensemble des salariés de l'industrie, du commerce et de l'artisanat. D'autre part, la LTr visait à adapter le droit en vigueur dans le domaine de la protection des travailleurs aux conditions et aux besoins « actuels »[659]. À cette fin, le Législateur a, entre autres, introduit l'art. 6 LTr qui se lit comme suit :

> « Pour protéger la santé des travailleurs, l'employeur est tenu de prendre toutes les mesures dont l'expérience a démontré la nécessité, que l'état de la technique permet d'appliquer et qui sont adaptées aux conditions d'exploitation de l'entreprise. Il doit en outre prendre toutes les mesures nécessaires pour protéger l'intégrité personnelle des travailleurs ».

Il va sans dire que la protection des travailleurs face aux risques liés à l'évaluation automatisée de certains aspects de leur personnalité ne faisait pas

656 Il en va autrement, à titre d'exemple, en Autriche, en France ou en Norvège où les Législateurs respectifs ont prévu une interdiction totale des analyses génétiques effectuées dans le cadre des relations de travail. L'Allemagne et le Portugal semblent connaître un régime similaire à celui qui a été prévu en Suisse. En revanche, en droit espagnol, rien n'a été prévu à ce sujet, voir FF 2017 5294.

657 Pour une analyse plus approfondie de cette Recommandation, voir *infra* Chapitre 12. Le cadre prévu par le Conseil de l'Europe.

658 Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce (Loi sur le travail, LTr) du 13 mars 1964, RS 822.11.

659 FF 1960 II 890 ; pour un aperçu de l'historique de cette loi, voir DUNAND/MAHON/WITZIG, pp. 6 ss.

partie des considérations du Législateur suisse de l'époque[660]. Depuis le début des années 2000, le Législateur s'est intéressé à la libéralisation des heures d'ouverture de certains types de magasins et a apporté, par voie d'ordonnance, quelques modifications ponctuelles à la protection des travailleurs, notamment au droit des jeunes mères à allaiter pendant les heures de travail ou à l'enregistrement du temps de travail[661]. L'impact des nouvelles formes de traitements de données sur le lieu de travail ne semble cependant pas avoir préoccupé le Législateur[662].

Cela étant, on peut se demander si la formulation très vague de l'art. 6 LTr permettrait d'encadrer le profilage dans le cadre d'une procédure d'embauche. En effet, il est de jurisprudence constante que l'employeur doit non seulement protéger l'intégrité physique mais aussi l'intégrité psychique des travailleurs[663]. Il est également établi depuis longtemps que la surveillance porte atteinte à l'intégrité psychique de la personne surveillée[664]. Le profilage étant une forme de surveillance, reste à savoir quelles mesures devraient être considérées comme « nécessaires pour protéger l'intégrité personnelle des travailleurs » et dès lors être mises en place par l'employeur.

Toutefois, avant de pouvoir répondre à cette question, il convient de déterminer si la LTr et l'Ordonnance 3 relative à la loi sur le travail[665] (ci-après « OLT 3 »), qui apporte des précisions en matière de surveillance sur le lieu de travail sont applicables à une procédure d'embauche. En effet, la détermination du champ d'application de la LTr peut s'avérer complexe[666]. Dans ce contexte, trois points méritent d'être rappelés.

660 Pour un résumé de ces révisions, voir FARNER, Introduction à la LTr, N 36 ss. ; dans le contexte de la présente contribution, on soulignera qu'au début des années 1980 déjà, certains auteurs regrettaient que le cadre légal des traitements de données personnelles effectués sur le lieu de travail n'ait pas suscité plus d'attention de la part de la doctrine et des tribunaux, voir TRUTMANN, pp. 466 et 468.

661 Art. 60, respectivement 73*a* et 73*b* Ordonnance 1 relative à la loi sur le travail.

662 À titre d'exemple, le *think tank* suisse *Reatch* a reconnu cette lacune et a lancé, dès 2017, plusieurs projets de sensibilisation relatifs aux futures relations de travail, voir Reatch, Zukunft der Arbeit, Wie wirkt sich der technologische und gesellschaftliche Wandel auf unsere Arbeit aus?, non daté, non encore traduit en français ; l'implémentation de nouvelles formes de surveillance due à la généralisation du télétravail suite à la pandémie du Covid-19 pourrait avoir comme conséquence de lancer la discussion quant à un encadrement éventuellement plus accru de la surveillance sur le lieu de travail.

663 À titre d'exemple, voir NÖTZLI, art. 6 LTr, N 25 et 29 avec des mentions jurisprudentielles.

664 À titre d'exemple, voir SECO, Commentaire de l'art. 26 OLT 3, p. 1.

665 Ordonnance 3 relative à la loi sur le travail (Protection de la santé) du 18 août 1993, RS 822.113.

666 MÜLLER/MADUZ, art. 1er LTr, N 3 ; dans le même sens, voir BACHMANN, Remarques préliminaires relatives aux art. 1er à 5 LTr, N 1.

D'abord, la protection de la personnalité des travailleurs, déjà ancrée à l'art. 328 CO, s'étend par l'art. 6 LTr au droit public du travail[667]. Il découle de cette constatation que la protection de la personnalité garantie par la LTr et celle offerte par le CO sont, en principe, identiques. Toutefois, il se peut que dans certaines hypothèses, la protection telle que prévue à l'art. 328 CO soit plus généreuse que celle fixée à l'art. 6 LTr, notamment lorsqu'il s'avère que les travailleurs nécessitent une protection particulière dans un cas précis[668]. Comme nous l'avons déjà vu plus haut[669], il n'est pas certain que l'art. 328 CO s'applique également aux procédures d'embauche. Dès lors, il ne semble pas justifié de proposer une interprétation généreuse du champ d'application de la LTr tant que le champ d'application *ratione temporis* de l'art. 328 CO n'a pas été clarifié (le champ d'application de la LTr peut être plus restreint, voire aussi large que celui du CO, mais pas plus large que celui du CO).

Ensuite, force est de constater que la LTr ne définit pas la notion de « travailleur » pourtant déterminante pour délimiter le champ d'application *ratione personae* de cette loi. L'art. 1 al. 1er de l'Ordonnance 1 relative à la loi sur le travail[670] (ci-après « OLT 1 ») fixe toutefois que « par travailleur on entend toute personne occupée dans une entreprise soumise à la loi, de manière durable ou temporaire, durant tout ou partie de l'horaire de travail »[671]. Au vu de cette disposition, il ne semble pas que le candidat puisse être assimilé à un « travailleur » au sens de la LTr.

Enfin, dans une veine plus abstraite, il convient de rappeler la *ratio legis* de la L Tr. La LTr avait pour but d'étendre le champ d'application *ratione personae* de la protection des travailleurs et visait, par-là, à améliorer la protection des travailleurs sur le lieu de travail, notamment grâce à l'introduction de l'art. 6 LTr. Cette disposition n'avait pas pour but d'étendre les obligations de l'employeur à la procédure d'embauche. Reprenant la logique de la LTr, il est en effet difficilement concevable qu'un employeur soit tenu responsable de garantir l'intégrité psychique d'une personne avec laquelle il n'a pas encore entamé de relation contractuelle.

667 La consécration de cette protection en droit public du travail permet au travailleur de directement s'adresser aux autorités chargées de l'exécution de la LTr, c'est-à-dire sans devoir s'adresser à l'employeur (art. 41 et 42 LTr). Par ailleurs, cette consécration a pour conséquence qu'il n'est pas admis de déroger à cette disposition.

668 NÖTZLI, art. 6 LTr, N 14.

669 Voir *supra* Chapitre 7. Le Code des obligations.

670 Ordonnance 1 relative à la loi sur le travail du 10 mai 2000, RS 822.111.

671 À juste titre, MÜLLER et MADUZ font valoir que cette définition est trop générale, voir MÜLLER/MADUZ, art. 1er LTr, N 8.

Il ressort de ces quelques développements qu'il semble très difficile, voire impossible d'étendre le champ d'application de l'art. 6 LTr à la phase précontractuelle du contrat de travail. Si d'un point de vue strictement juridique, une telle conclusion s'impose, elle est regrettable au vu des enjeux du profilage pour l'intégrité des candidats. Conscient de l'impact des mesures de surveillance sur la santé mentale, le SECO prend explicitement position par rapport à l'encadrement de diverses formes de surveillance *pendant* la relation de travail[672]. Toutefois, le profilage mis en place *avant* la conclusion du contrat de travail reste non-encadré par les dispositions de droit public censées garantir la santé (mentale) dans le monde du travail. Reste alors à se demander si un employeur qui a recours au profilage pourrait, dans certaines circonstances, faire face à une sanction de nature pénale.

E. L'encadrement pénal du profilage

D'un point de vue pénal, l'art. 61 let. b et/ou let. c LPD (1) et l'art. 179novies du Code pénal[673] (ci-après « CP ») (2) pourraient potentiellement trouver application lorsqu'un employeur procède à un profilage d'un candidat. Dès lors, il convient de brièvement analyser le champ d'application de ces deux articles relevant du droit pénal accessoire.

1. La violation des devoirs de diligence (art. 61 let. b et c LPD)

A titre préliminaire, il convient de noter que le dispositif pénal de l'aLPD devait être renforcé dans le cadre de la révision, notamment en raison des exigences de la Convention 108+ et du RGPD. Un système pénal trop clément aurait en effet pu avoir comme conséquence que la réglementation suisse ne soit plus jugée suffisante par l'UE et que par conséquent, l'UE refuse d'octroyer la décision d'adéquation à la Suisse[674]. En vue d'obtenir cette décision d'adéquation, le Législateur suisse s'est donc vu dans l'obligation de renforcer le dispositif pénal de la LPD sans toutefois reprendre le régime prévu dans le RGPD ou la

672 En pratique, le Commentaire de l'ordonnance 3 relative à la loi sur le travail a une portée importante, voir SECO, Commentaire de l'art. 26 OLT 3 ; il convient de noter que dans sa version actuelle, ce document ne mentionne pas le profilage comme un des multiples exemples de surveillance sur le lieu de travail. Toutefois, ce document est en voie de révision et il a été du vœu du PFPDT que dans la version révisée du commentaire, le profilage soit mentionné comme un exemple de mesure de surveillance potentiellement illicite. Il est à espérer que les responsables de la révision incorporeront la prise de position du PFPDT.

673 Code pénal suisse du 21 décembre 1937, RS 311.0.

674 FF 2017 6714 s. ; contrairement au Conseil fédéral, MÖHLE est d'avis que le régime pénal ne fait pas partie des multiples critères qui seront pris en compte lors de cette décision d'adéquation, voir MÖHLE, pp. 599 ss.

Convention 108+ dans leur totalité. Ainsi, le dispositif pénal de la LPD révisée se distingue du dispositif pénal européen sur trois points essentiels :

— les amendes sont limitées à 250'000 francs suisses (contrairement à une limite fixée à 20 millions d'euros ou à 4 % du chiffre d'affaires mondial en droit européen) et sont prononcées, le cas échéant, à l'encontre d'une personne physique (contrairement au droit européen qui prévoit de sanctionner la personne morale responsable du traitement de données illicite) ;
— le droit suisse sanctionne uniquement les violations intentionnelles de la LPD ;
— le nombre d'infractions est considérablement plus faible qu'en droit européen[675].

Dans ce contexte, le Législateur suisse a, entre autres, également introduit le nouvel art. 61 let. b et c LPD dans la mesure où la LPD révisée prévoit de nouvelles obligations élémentaires qui n'étaient pas couvertes par les dispositions pénales en vigueur sous le régime de l'aLPD[676]. Ainsi, afin de mieux protéger la personnalité des personnes concernées, cette disposition se lit comme suit :

Sont, sur plainte, punies d'une amende de 250'000 francs au plus les personnes physiques privées qui, intentionnellement (...) :

b. confient le traitement de données personnelles à un sous-traitant sans que les conditions de l'art. 9, al. 1 et 2, soient remplies ;

c. ne respectent pas les exigences minimales en matière de sécurité des données édictées par le Conseil fédéral selon l'art. 8, al. 3.

À la lumière de ces deux alinéas, il convient de relever deux aspects d'ordre abstrait.

D'abord, le sous-traitant ne semble pas risquer une quelconque poursuite pénale sur la base de cette disposition[677]. Ainsi, il incombe au responsable du traitement de s'assurer que le sous-traitant respecte ce qui a pu être fixé dans le contrat de sous-traitance.

Ensuite, il semble que les exigences liées à la sécurité des données n'ont pas subi de modifications matérielles à la suite de la révision[678]. Au regard des débats complexes qui ont eu lieu dans le cadre de la consultation des offices, il n'est pourtant pas certain que cette affirmation de ROSENTHAL soit pertinente.

675 ROSENTHAL, Das neue Datenschutzgesetz, N 191 s.

676 FF 2017 6716.

677 À mon sens, à juste titre, voir ROSENTHAL, Das neue Datenschutzgesetz, N 61 ; pour une position plus vague quant à cette question, voir FF 2017 6716.

678 ROSENTHAL, Das neue Datenschutzgesetz, N 53 ; voir, pour les détails, art. 8 aOLPD et 1 OPDo respectivement, et OFJ, Rapport explicatif sur la révision de l'ordonnance sur la protection des données du 31 août 2022, pp. 18 ss., et, plus spécifiquement par rapport à la violation des devoirs de diligence au sens de l'art. 61 let. c LPD, voir p. 21.

Dans une veine plus concrète, on peut se demander dans quelle mesure cette nouvelle disposition vient encadrer un profilage effectué dans le cadre d'une procédure d'embauche. Plusieurs points méritent d'être soulevés à ce sujet.

Contrairement à ce qui a pu être fixé en droit européen et à ce que le PFPDT aurait souhaité[679], le Législateur suisse a renoncé à sanctionner le responsable du traitement qui violerait ses obligations par négligence. Or, le plus souvent, les atteintes au droit de la personnalité sont commises par négligence, notamment en raison d'une sensibilisation insuffisante. Ce choix du Législateur a donc pour conséquence de réduire le nombre d'hypothèses dans lesquelles une autorité de poursuite pénale interviendra à l'encontre d'un employeur trop peu soucieux de la protection des données.

On peut relever ensuite que l'infraction est poursuivie sur plainte uniquement. Il est peu probable qu'un candidat qui a obtenu la place de travail aille porter plainte contre son nouvel employeur. De même, et à condition qu'il ait en effet eu connaissance du fait qu'il a fait l'objet d'un profilage, un candidat qui n'a pas été retenu ne va très probablement pas déposer plainte. En vertu de l'art. 62 al. 2 LPD, le PFPDT peut dénoncer des infractions aux autorités de poursuite pénale compétentes et faire valoir les droits d'une partie plaignante dans la procédure. Cela étant, au regard de sa taille modeste, il semble peu probable que les collaborateurs du PFPDT soient disposés à intervenir souvent. En revanche, le PFPDT ne peut ni sanctionner une violation du droit de la protection des données qu'il constaterait par son enquête ni le non-respect de ses propres décisions contraignantes[680]. En d'autres termes, le fait que l'art. 61 LPD limite la poursuite pénale aux cas dénoncés risque de considérablement restreindre la portée de cette disposition en pratique.

De surcroît, même s'il est vrai que 250'000 francs suisses peuvent représenter une somme considérable pour une personne physique, il n'est pas certain que cette somme limite l'appétit des employeurs à en savoir toujours plus à propos des candidats[681], d'autant plus que la plupart des profilages sont effectués à l'insu des personnes concernées. L'effet dissuasif de la sanction doit dès lors être considéré comme nul.

679 FF 2017 6715.

680 FF 2017 6719 ; très critique, voir MÉTILLE, La (nouvelle) loi fédérale, p. 40 et, déjà à propos de l'avant-projet, précisant que le fait que le PFPDT ne dispose d'aucun pouvoir de sanction « s'inscrit à contre-courant du régime européen et pourrait bien ne pas être conforme à la Convention 108 du Conseil de l'Europe », voir MÉTILLE/RAEDLER, pp. 38 s. ; moins critique, mais précisant que pour cette raison, la disposition risque de rester lettre morte, voir ROSENTHAL, Das neue Datenschutzgesetz, N 193.

681 Le PFPDT est du même avis, voir FF 2017 6715 ; pour l'avis contraire, voir ROSENTHAL, Das neue Datenschutzgesetz, N 191 s.

D’ailleurs, il convient de rappeler que les autorités compétentes sont les autorités de poursuite cantonales[682]. Or, ces autorités cantonales n’ont que peu d’expérience quant au volet pénal du droit de la protection des données[683]. De plus, une compétence cantonale en la matière semble aller à l’encontre d’une application uniforme du droit de la protection des données. Une application uniforme de cette matière est pourtant nécessaire dans un monde économique interconnecté. Reste à savoir si les autorités cantonales sauront relever ce défi – à condition bien évidemment qu’un candidat soumis à un profilage saisisse la justice pénale.

En conclusion, cette disposition risque de rester lettre morte dans les hypothèses qui nous intéressent dans le cadre de la présente contribution. Dès lors, il convient de se demander si une disposition figurant dans le CP pourrait éventuellement trouver application lorsqu’un employeur effectue un profilage d’un candidat.

2. La soustraction de données personnelles (art. 179^{novies} CP)

Introduit en 1992 par l’annexe de l’aLPD[684] et légèrement modifié avec l’entrée en vigueur de la LPD révisée, l’art. 179^{novies} CP prévoit que « celui qui aura soustrait des données personnelles sensibles qui ne sont pas accessibles à tout un chacun sera, sur plainte, puni d’une peine privative de liberté de trois ans au plus ou d’une peine pécuniaire ».

Dans le cadre de la révision de la LPD, la notion de « profil de la personnalité » a été abrogée. Plusieurs lois fédérales qui reprenaient cette notion, comme p. ex. le CP, ont donc dû être adaptées. La notion de « profil de la personnalité » et celle de « profilage » se ressemblent, mais ne se recoupent pas entièrement. La notion de « profil de la personnalité » mentionnée à l’art. 179^{novies} CP avant la révision de la LPD n’a dès lors pas été remplacée par celle de « profilage ». Seule la soustraction de données personnelles sensibles peut dès lors être sanctionnée pénalement.

De même, la notion de « fichier » a été éliminée de cette disposition pénale. En effet, une telle modification s’imposait dans la mesure où « compte tenu des nouvelles technologies, les données peuvent aujourd’hui être exploitées comme un fichier, alors même qu’elles sont disséminées. Un exemple parlant est le profilage, lors duquel on va chercher des données dans différentes sources, non constitutives de fichiers, afin d’évaluer certaines caractéristiques d’une personne »[685].

682 Art. 65 al. 1er LPD.

683 À juste titre, voir ROSENTHAL, Das neue Datenschutzgesetz, N 193.

684 Au même titre, par exemple, que l’art. 328b CO.

685 FF 2017 6643 s.

Enfin, la nouvelle disposition remplace le bout de phrase « [les données personnelles sensibles] qui ne sont pas librement accessibles » par « [les données personnelles sensibles] qui ne sont pas accessibles à tout un chacun »[686]. Le Message du Conseil fédéral étant dépourvu de toute précision à cet égard, il semble que ce changement terminologique n'entraîne aucune modification matérielle.

Dans une veine abstraite, on retiendra que cette disposition vient protéger la personnalité de la personne dont les données personnelles sensibles ont été soustraites[687] et non le patrimoine du responsable du traitement[688]. De plus, la notion de « données personnelles sensibles » renvoie à la définition légale telle que prévue à l'art. 5 let. c LPD[689]. La simple prise de connaissance de données personnelles sensibles peut, à mon sens à juste titre, constituer une soustraction au sens de l'art. 179^{novies} CP dans la mesure où une telle prise de connaissance suffit à porter atteinte à la personnalité de la personne concernée[690]. L'auteur de l'infraction peut, ensuite, soustraire des « données personnelles sensibles qui ne sont pas accessibles à tout un chacun [...] de différentes manières : il peut dérober des dossiers entiers ou une partie de ceux-ci, il peut s'introduire dans le système à partir d'un terminal, ou encore il peut intercepter des transmissions de données »[691]. Il est regrettable que le Message du Conseil fédéral de 2017 reste muet à propos des modifications apportées à l'art. 179^{novies} CP dans le cadre de la révision de la LPD. En effet, les exemples cités datent de 1988 et ne reflètent pas les pratiques des *data broker* au 21ème siècle. La pratique d'acheter des données ou d'effectuer de vastes recherches dans diverses bases de données afin de procéder à des évaluations statistiques automatisées ne semble pas être couverte par les Messages du Conseil fédéral. Ensuite, l'auteur de l'infraction n'est punissable que s'il a agi intentionnellement. Enfin, on rappellera qu'il s'agit d'un délit qui n'est poursuivi que sur plainte. Il ne fait aucun doute que la personne concernée peut porter plainte. Toutefois, sur la question du dépôt ou non d'une plainte par le responsable du traitement de données la doctrine est partagée[692]. À la

686 FF 2017 6741.

687 TRECHSEL/LIEBER, art. 179^{novies} CP, N 1 ; dans le même sens, voir DONATSCH, art. 179^{novies} CP, N 1.

688 FF 1988 II 496.

689 FF 1988 II 496.

690 TRECHSEL/LIEBER, art. 179^{novies} CP, N 6 ; dans le même sens, voir DONATSCH, art. 179^{novies} CP, N 6 ; dans le sens contraire, voir ARZT, art. 179^{novies} CP, N 12 ; pour une position peu claire, voir WOHLERS, art. 179^{novies} CP, N 2.

691 FF 1988 II 496.

692 Pour une réponse affirmative à cette question, voir FF 1988 II 496 et DONATSCH, art. 179^{novies} CP, N 8 ; pour une analyse plus réservée, voir TRECHSEL/LIEBER, art. 179^{novies} CP, N 7 ; pour une proposition de soumettre la validité de la plainte à une plainte conjointe, voir ARZT, art. 179^{novies} CP, N 15.

lumière du bien juridique protégé par cette disposition, il semble qu'une réponse restrictive à cette dernière question s'impose.

À l'aune de ces développements abstraits, il convient de soulever quelques aspects qui pourraient s'avérer problématiques lorsqu'il s'agit d'appliquer cet article dans le contexte d'une procédure d'embauche.

À titre préliminaire, il convient de rappeler que l'employeur qui ne procéderait pas lui-même au profilage en déléguant cette tâche à un *data broker* reste responsable du traitement au sens de l'art. 5 let. j LPD. Il découle de cette constatation qu'il peut, entre autres, engager sa responsabilité pénale, notamment en procédant à un traitement de données interdit par la loi pénale[693].

Force est de constater, tout d'abord, que cette disposition pénale s'applique uniquement à la soustraction de données personnelles sensibles qui ne sont pas accessibles à tout un chacun. Or, comme nous l'avons vu plus haut, un profilage peut sans autre se fonder sur des données personnelles non-sensibles, voire anonymes qui sont librement accessibles. À première vue, l'employeur qui effectue un profilage ne semble dès lors pas courir un grand risque d'être poursuivi pénalement. Toutefois, il est fort probable que dans le cadre d'une évaluation automatisée de données non-sensibles de nouvelles données sensibles émergent, notamment sur la base d'une corrélation inattendue. Au vu de la lettre de la loi, il n'est pas établi que cette disposition couvre l'hypothèse d'un tel profilage.

Ensuite, un employeur qui mandate un *data broker*, afin que ce dernier procède à l'évaluation d'un candidat, le fera dans le but d'avoir accès à des informations qui ne lui sont pas autrement accessibles. En d'autres termes, l'employeur mandate le *data broker* afin de prendre connaissance de certaines données personnelles qui ne sont pas accessibles à tout un chacun. L'existence de ce deuxième élément constitutif du délit doit donc également être constatée.

Ensuite, si une interprétation large de la notion de « soustraction » est retenue, le profilage d'un candidat remplira le troisième élément constitutif du délit dans la mesure où le profilage n'a qu'un sens si l'employeur peut en prendre connaissance une fois le traitement de données effectué.

Enfin, reste à savoir si l'employeur, qui mandate un des multiples *data broker* afin d'optimiser la gestion des dossiers de candidature agit intentionnellement au sens de l'art. 12 CP. Dans ce contexte, il pourrait s'avérer compliqué de retenir l'intention délictueuse dans la mesure où, faut de sensibilisation, la plupart des employeurs effectueront un profilage après avoir répondu à une offre d'un *data broker* en toute bonne foi.

693 Dans le même sens à propos de l'art. 61 let. b et c LPD, voir *supra* Chapitre 9. Autres dispositifs fédéraux potentiellement applicables.

Cela étant, il convient de noter que l'employeur ne sera puni que sur plainte. Il est peu probable qu'un candidat qui a obtenu la place de travail aille porter plainte contre son nouvel employeur ; un candidat qui n'a pas été retenu (à condition qu'il ait connaissance du fait qu'il a fait l'objet d'un profilage) ne va très probablement pas – pour d'autres raisons bien évidemment – déposer plainte. Pour des raisons liées non seulement aux éléments constitutifs du délit mais aussi à cet aspect procédural, cette disposition risque donc de rester lettre morte dans le contexte de procédures d'embauche.

La portée de cette disposition semble non seulement être limitée dans le cadre d'une procédure d'embauche, mais aussi d'une manière plus générale. En effet, il n'existe qu'un seul arrêt du Tribunal fédéral publié au recueil officiel dans le cadre duquel cette disposition a trouvé application (parmi d'autres dispositions pénales)[694]. Dans cette affaire, il s'agissait d'une avocate qui s'était adressée, dans le cadre d'une procédure de divorce, au tribunal afin d'avoir accès aux documents concernant la partie adverse (le plaignant). Le secrétaire du tribunal concerné avait transmis ces documents à l'avocate qui avait, grâce aux informations figurant dans ces documents, pu prendre connaissance de plusieurs peines pénales prononcées à l'encontre du plaignant et ainsi procurer un avantage stratégique à sa cliente. Les faits jugés dans cette affaire se distinguent donc des constellations discutées dans cette contribution.

Les autres dispositions pénales consacrées aux infractions contre le domaine secret ou le domaine privé ne semblent pas être applicables dans l'hypothèse d'un profilage dans le cadre d'une procédure d'embauche. Toutefois, il convient de ne pas oublier que l'une ou l'autre de ces dispositions pourraient trouver application lorsque l'employeur effectue un profilage *pendant* la relation de travail. On pensera notamment aux art. 179 CP (violation de secrets privés), 179bis CP (écoute et enregistrement de conversations entre d'autres personnes), 179ter CP (enregistrement non autorisé de conversations) et 179^{quater} CP (violation du domaine secret ou du domaine privé au moyen d'appareil de prise de vues).

F. Un encadrement lacunaire

Il découle des paragraphes précédents que tant la LTr que la LHand ne sont pas applicables aux procédures d'embauche régies par le droit privé. Les champs d'application de la LEg et de la LAGH couvrent les procédures d'embauche. Toutefois, ces deux lois fédérales n'encadrent que certains traitements de données personnelles très spécifiques. Les dispositions pénales semblent

694 ATF 122 IV 139.

dénuées d'effet dissuasif et risquent de rester lettre morte en raison de diverses aspects problématiques liés à leur mise en œuvre. Ainsi, sur la base des développements mis en avant aux chapitres 7 et 8, qui ont pu montrer que le CO et la LPD n'encadraient que très partiellement le profilage, il convient de clore ce neuvième chapitre en constatant que les divers autres dispositifs fédéraux qui auraient potentiellement pu encadrer ce traitement de données n'offrent qu'une protection lacunaire des droits des candidats soumis au profilage.

Chapitre 10.
Conclusion de la deuxième partie

Cette deuxième partie avait pour but de chercher à savoir si un profilage effectué par un employeur établi en Suisse était licite en vertu des différentes lois fédérales applicables et quelles étaient, le cas échéant, les limites imposées à l'employeur par le régime légal en vigueur. En guise de réponse à ces deux questions soulevées au début de cette contribution, on retiendra les points suivants :

À travers l'art. 328 CO, les droits fondamentaux des candidats peuvent déployer certains effets entre particuliers. De plus, la formulation très ouverte de cette disposition permet d'adapter son champ d'application aux développements de la société, p. ex. d'ordre technologique. Toutefois, la doctrine n'est pas unanime sur l'applicabilité de cette disposition à la procédure d'embauche. Une jurisprudence constante en la matière fait défaut. L'articulation entre l'art. 328b CO, qui encadre les traitements qui peuvent être effectués lors de la procédure d'embauche, et les dispositions générales de la LPD doivent encore faire l'objet de clarifications jurisprudentielles. Au regard des dispositions pertinentes du CO, on ne peut clairement affirmer que le profilage est licite.

Ensuite, on retiendra que plusieurs éléments de la notion de profilage d'une part et de profilage à risque élevé d'autre part telles que prévues dans la LPD révisée restent peu clairs. Les contours de ces deux notions devront donc être clarifiés. Cela étant, on notera que le profilage viole systématiquement le principe de proportionnalité ainsi que le principe de finalité tels qu'entendus actuellement. D'autres principes généraux comme p. ex. le principe de la bonne foi, le principe de l'exactitude ou de la transparence peuvent également être violés lors d'un profilage effectué par un employeur au stade de la procédure d'embauche. On rappellera qu'une violation d'un principe général peut être justifiée. Ni une loi ni un intérêt prépondérant public ni le consentement du candidat ne sont pertinents dans le cas d'espèce. Il est très peu certain que l'intérêt prépondérant de l'employeur puisse justifier le profilage.

Les mesures d'ordre technique, voire d'ordre organisationnel reprises de l'aLPD (registre des activités de traitement, certification) ou nouvellement introduites lors de la révision (protection des données dès la conception ou par défaut, analyse d'impact, codes de conduite) ne contribueront pas à garantir une meilleure protection des droits des candidats.

En bref, un profilage effectué par un employeur au stade de la procédure d'embauche viole systématiquement la LPD. Ces violations ne seront toutefois que peu, voire jamais invoquées devant une autorité judiciaire, notamment en raison de l'opacité qui entoure le profilage, les ressources (très) restreintes de l'autorité de surveillance et des moyens de droit inadaptés au profilage.

Il ne fait aucun doute que la LEg est applicable à la procédure d'embauche. Toutefois, le renversement du fardeau de la preuve ne trouve pas application au stade du recrutement. De plus, le droit à l'explication écrite à la suite d'un profilage n'est pas un moyen adéquat permettant de comprendre puis, le cas échéant, contester le raisonnement de l'évaluation automatisée. On notera également que la LEg n'offre qu'une protection dans les cas où il s'agirait d'un profilage qui aurait conduit à une discrimination sur la base du sexe. Ainsi, au vu de la quantité et de la diversité des données traitées lors d'un profilage, la plupart des profilages ne devraient pas tomber dans le champ d'application de cette loi.

Il en va de même de la LAGH qui propose un régime très nuancé dont le respect est surveillé par les inspecteurs du travail cantonaux. Le champ d'application de la LAGH reste toutefois limité aux profilages qui sont effectués dans le cadre d'analyses génétiques humaines.

La LTr et la LHand quant à elles ne sont pas applicables aux procédures d'embauche soumises au droit privé.

Enfin, s'il est vrai que le régime pénal a été renforcé dans le cadre de la révision, force est de constater que les infractions ne seront poursuivies sur plainte seulement, que les infractions commises par négligence ne seront pas poursuivies et que les sanctions restent très peu dissuasives. En d'autres termes, le régime pénal risque de rester lettre morte.

Ainsi, les différentes lois fédérales potentiellement applicables au cas d'espèce ne semblent pas être en mesure de protéger le droit de la personnalité des candidats ainsi que leurs intérêts, que les droits fondamentaux ont pour objet de protéger. Dès lors, il convient de se pencher sur la garantie constitutionnelle qui sous-tend le droit de la protection des données afin de déterminer si elle pourrait, voire devrait être appliquée de manière plus extensive afin de combler les lacunes juridiques décrites tout au long de cette deuxième partie.

Partie 3. Le cadre constitutionnel du profilage

Parmi les divers droits fondamentaux qui peuvent trouver application lorsqu'un particulier effectue un traitement de données, le droit à une protection contre l'emploi abusif de données personnelles consacré à l'art. 13 al. 2 Cst. est au cœur de la protection constitutionnelle des données personnelles. Lorsque le Tribunal fédéral est amené à interpréter cette disposition constitutionnelle, la jurisprudence de Strasbourg exerce une influence toute particulière sur sa prise de décision. En effet, en matière de protection des données, la plus haute juridiction suisse s'inspire souvent des arrêts de la Cour EDH, notamment lorsqu'elle est amenée à déterminer si et dans quelle mesure l'art. 13 al. 2 Cst. doit également trouver application entre particuliers[695].

Dès lors, il convient, dans un premier temps, de se pencher sur les éventuelles limites imposées aux responsables du traitement de données personnelles soumis au droit privé qui découlent de l'art. 13 al. 2 Cst. (chapitre 11) avant d'examiner la jurisprudence pertinente de la Cour EDH (chapitre 12). Contrairement au Conseil de l'Europe, l'Union européenne a expressément consacré le droit à la protection des données à caractère personnel à l'art. 8 de la Charte des droits fondamentaux. Une analyse de cet aspect du cadre « constitutionnel européen »[696] s'impose pour éventuellement s'en inspirer lors de toute réflexion ultérieure portant sur une possible amélioration de l'encadrement des traitements de données effectués par des particuliers en Suisse (chapitre 13). Le dernier chapitre de cette troisième partie offrira un résumé de l'analyse du cadre constitutionnel (chapitre 14).

695 SCHWEIZER R., Rechtsprechung des EGMR, pp. 462 s.

696 Expression reprise de BESSON, pour un aperçu des autres aspects constitutionnels du droit européen, voir BESSON, Droit constitutionnel européen, N 99.

Chapitre 11.
Le cadre constitutionnel suisse

Afin de mieux comprendre le cadre constitutionnel prévu par l'art. 13 al. 2 Cst., quelques remarques préliminaires s'imposent (A). Après avoir déterminé si l'art. 13 al. 2 Cst. a un rôle à jouer entre privés (B), la portée (potentielle) de cette disposition dans le cadre d'une procédure d'embauche devra faire l'objet d'une analyse approfondie (C). Ce chapitre se terminera par une brève conclusion, qui retracera les arguments développés (D).

A. Quelques remarques préliminaires

La protection constitutionnelle contre tout traitement de données personnelles abusif telle que prévue à l'art. 13 al. 2 Cst.[697] est une composante de la garantie constitutionnelle du droit au respect de la vie privée et familiale telle que consacrée à l'art. 13 al. 1er Cst.[698], qui est elle-même une composante de la protection constitutionnelle de la liberté personnelle fixée à l'art. 10 al. 2 Cst[699].

Bien que l'art. 13 al. 2 Cst. ne mentionne pas le droit à l'autodétermination en matière informationnelle (*informationelles Selbstbestimmungsrecht*), il est généralement admis que cette disposition garantit ce droit[700] qui peut être décrit[701] comme « le droit de ne pas accepter un traitement qui ne correspond pas

697 Littéralement, l'art. 13 al. 2 Cst. garantit que « toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent ».

698 Pour des précisions quant à la distinction entre ces deux garanties constitutionnelles, voir BELSER, § 6, N 162 ss.

699 À titre informatif, il convient de rappeler que la doctrine n'est pas unanime concernant les garanties constitutionnelles qui constituent la liberté personnelle. À titre d'exemple, MOECKLI mentionne les art. 10 al. 2, 13 et 31 Cst., voir MOECKLI, N 7. BELSER fonde la liberté personnelle sur les art. 10 al. 2, 13 et 7 Cst., voir BELSER, § 6, N 14. Tous s'accordent néanmoins à reconnaître que l'art. 13 Cst. est une composante de l'art. 10 al. 2 Cst. Une analyse plus approfondie des composantes de la liberté personnelle dépasserait toutefois le cadre de cette contribution.

700 MEIER, Protection des données, N 17 ; HERTIG RANDALL/MARQUIS, art. 13 Cst., N 62 ; BELSER, § 6, N 60 ; MOECKLI, N 37 ; DIGGELMANN, art. 13 Cst., N 32 ; MONTAVON, pp. 662 ss.

701 Le choix du verbe est déterminant. En effet, le droit à l'autodétermination en matière informationnelle n'a jamais été *défini*, voir, pour plus de détails, FLÜCKIGER, p. 847 ou FASNACHT, N 111 ss.

à la volonté exprimée [de la personne concernée] »[702], voire « garantit [...] que l'individu demeure maître de ses données personnelles »[703]. Ce droit a été mentionné pour la première fois par la Cour constitutionnelle allemande dans son célèbre arrêt de 1983[704] (*Volkszählungsurteil*)[705] avant d'être repris par le Tribunal fédéral en tant que droit constitutionnel non-écrit dans deux arrêts rendus en 1987[706] puis développé[707]. Ce droit n'a été consacré en tant que droit fondamental écrit qu'en 1999 lors de la révision totale de la Cst.[708]. Avant l'entrée en vigueur de la Cst. révisée, la protection des données personnelles était également garantie par le biais de l'art. 8 CEDH[709].

Le droit à l'autodétermination en matière informationnelle a depuis toujours été considéré comme le droit constitutionnel le plus apte à répondre aux défis imposés par les développements technologiques[710]. En raison de ces développements et des utilisations très variées qui peuvent être faites des nouvelles formes de traitements de données[711], les contours de cette garantie constitutionnelle sont en permanente évolution[712]. À juste titre, le Tribunal

702 MEIER, Protection des données, N 17 avec de multiples références supplémentaires ; dans une veine similaire, FASNACHT estime que l'autodétermination en matière informationnelle signifie que « [traduction] les personnes concernées peuvent décider elles-mêmes qui traite leurs données personnelles, quand et dans quelles circonstances », voir FASNACHT, N 99.

703 HERTIG RANDALL/MARQUIS, art. 13 al. 2 Cst., N 62 ; dans le même sens, voir FÜZESSÉRY/SCHNEIDER, p. 154.

704 BVerfGE 65, 1.

705 Pour un résumé de cet arrêt en français, voir MONTAVON, p. 663.

706 Dans ce contexte, la doctrine s'accorde à citer les ATF 113 Ia 1 et 113 Ia 257, voir FLÜCKIGER, p. 849 ou SCHWEIZER R., art. 13 al. 2 Cst., N 39 ; BELSER émet des critiques quant à la reprise, en droit suisse, d'une notion étrangère au droit constitutionnel helvétique en précisant qu' « [traduction] alors que la Constitution allemande garantit la 'capacité civile générale' (*allgemeine Handlungsfähigkeit*) en tant que droit fondamental (et qu'il était donc logique de donner certains effets à cette capacité civile dans le contexte de traitements de données), la Constitution suisse ne consacre pas une telle 'capacité civile générale', mais protège uniquement les manifestations élémentaires du développement de la personnalité dans le cadre de la liberté personnelle », voir BELSER, § 6, N 119.

707 On notera que ce n'est qu'en 1994 qu'apparaît expressément la notion de « droit à l'autodétermination en matière informationnelle », notamment dans le cadre d'un litige de droit privé opposant un employé à son employeur qui lui refusait l'accès à son dossier personnel, voir ATF 120 II 118 ; pour un résumé détaillé des développements jurisprudentiels en la matière, voir FLÜCKIGER, pp. 849 ss. ou, plus critique, FASNACHT, N 104 ss.

708 MOECKLI, N 5.

709 MEIER, Protection des données, N 16 s.

710 FLÜCKIGER, p. 837.

711 Pour un aperçu de ces utilisations très variées, voir, à titre d'exemple, FLÜCKIGER, p. 838.

712 GONIN, N 2092.

fédéral a donc renoncé à adopter une quelconque définition de ce droit constitutionnel. Au contraire, il se contente de décrire ce droit en de termes plus ou moins vagues, voire d'adopter une approche casuistique[713]. Il convient de noter que ce faisant, la plus haute juridiction suisse s'inspire de la jurisprudence de la Cour EDH[714]. Cette constatation n'a cependant rien de surprenant vu que le droit fondamental au respect de la vie privée et familiale (dont découle, entre autres, le droit à la protection des données) est le seul droit fondamental qui a été consacré au niveau international *avant* d'être introduit dans les diverses constitutions libérales[715] et que si le Tribunal fédéral ne peut procéder à un contrôle de constitutionnalité des lois fédérales, il peut effectuer un contrôle de conventionnalité des dispositions fédérales litigieuses[716]. De surcroît, on précisera que « lorsque les particuliers invoquent l'application de cette convention, le Tribunal fédéral retient le sens que lui a donné la Cour [EDH], même lorsque les arrêts concernent des États tiers »[717]. Une analyse de ce droit fondamental ne saurait donc être complète sans prendre en considération la jurisprudence de la Cour EDH[718] et les diverses publications des organes internationaux compétents en la matière[719].

Aujourd'hui, au vu des défis posés par les développements technologiques, la question n'est pas si, mais plutôt quand le juge constitutionnel décidera d'étendre le champ d'application de cette disposition, voire de resserrer son

713 HERTIG RANDALL/MARQUIS, art. 13 Cst., N 20. À titre informatif, il convient de noter qu'il en va de même du droit constitutionnel au respect de la vie privée et familiale. En effet, malgré de nombreuses tentatives, une définition légale de ce droit fondamental n'a pas pu être trouvée, ni au niveau national ni au niveau international. La Cour EDH et le Tribunal fédéral adoptent donc également une approche casuistique lorsqu'ils se prononcent sur les contours du droit au respect de la vie privée et familiale, pour un aperçu de la littérature à ce sujet, voir DIGGELMANN/CLEIS, p. 442, n 6 ; pour un aperçu de la jurisprudence casuistique de la Cour EDH, voir EPINEY/SCHLEISS, § 3, N 9 ss.

714 HERTIG RANDALL/MARQUIS, art. 13 Cst., N 6.

715 MOECKLI, N 4 ; pour les raisons pour lesquelles les auteurs de la CEDH, de la Déclaration universelle des droits de l'homme et du Pacte II n'ont pas eu conscience, au sortir de la deuxième guerre mondiale, des conséquences de la consécration d'un tel droit fondamental au niveau international et de plus amples détails quant à cette évolution singulière, voir DIGGELMANN/CLEIS, pp. 441 ss.

716 À titre d'exemple, voir PÉTERMANN, pp. 14 ss. et tout particulièrement p. 24.

717 WERRO/SCHMIDLIN, pp. 172 s.

718 Pour un résumé des développements jurisprudentiels (jusqu'en 2009) de la Cour EDH en matière de protection des données, voir SCHWEIZER R., Rechtsprechung des EGMR, pp. 462 ss.

719 Pour des raisons de lisibilité, les développements jurisprudentiels de la Cour EDH et les éventuelles obligations qui en découlent pour l'ordre juridique suisse seront retracés dans le chapitre suivant, voir *infra* Chapitre 12. Le cadre prévu par le Conseil de l'Europe.

contrôle sous l'angle de la proportionnalité[720]. Dès lors, il convient de se demander si cette disposition est applicable aux relations entre particuliers avant de déterminer son éventuel (nouveau) champ d'application dans les relations entre un employeur privé et un candidat.

B. La portée de l'art. 13 al. 2 Cst. entre particuliers

En principe, les droits fondamentaux encadrent les relations juridiques qui lient les individus à l'État et ne trouvent, dès lors, pas application entre particuliers[721]. Plusieurs raisons peuvent être avancées à l'appui de cette approche. D'abord, les droits fondamentaux ont vocation à éviter toute nouvelle forme d'abus de pouvoir de la part des autorités publiques. D'un point de vue historique, les droits fondamentaux ne s'appliquent donc pas entre particuliers[722]. Ensuite, le contenu des droits fondamentaux ne se prête généralement pas à une application entre privés[723]. Après, si les particuliers pouvaient se prévaloir de leurs droits fondamentaux dans un rapport de droit privé, ils seraient souvent les deux à pouvoir opposer (à l'autre) une garantie constitutionnelle ce qui générerait des conflits de droits fondamentaux[724]. De surcroît, « les droits fondamentaux étant définis de manière très générale et très abstraite »[725], leur application directe à un rapport de droit privé serait source d'incertitudes et nuirait ainsi à la sécurité juridique. Enfin, « la possibilité pour la partie à un rapport de droit privé de se prévaloir directement des droits fondamentaux se heurterait à la maxime selon laquelle chaque particulier dispose de ses intérêts librement, en aménageant ses relations juridiques comme bon lui semble »[726] (principe de l'autonomie de la volonté).

720 HERTIG RANDALL/MARQUIS, art. 13 Cst., N 73 ; pour une approche allant dans le même sens, mais indépendante d'un ordre constitutionnel particulier, voir REHM, Digital Age, p. 378.

721 Art. 35 al. 2 Cst.

722 PULVER, p. 413 ; dans le même sens, voir BARAK, p. 17 ou WERRO/SCHMIDLIN, p. 177.

723 DUBEY, § 3, N 145 ; à ce sujet, BARAK précise que les droits fondamentaux ne sont pas absolus. À défaut de limites constitutionnelles prévues à l'application de ces droits entre particuliers, les droits fondamentaux ne se prêteraient qu'à une application entre l'État et les particuliers, les limites aux droits ainsi appliqués dans l'ordre juridique suisse étant fixées à l'art. 36 Cst., les limites aux droits entre particuliers devant être fixées dans des lois, voir BARAK, p. 17 ; d'un avis explicitement contraire, voir WERRO/SCHMIDLIN, pp. 180 s.

724 DUBEY, § 3, N 145 ; à ce sujet, BARAK précise qu'une application simultanée des droits fondamentaux de deux parties à un rapport de droit privé aurait pour conséquence ultime de les nier et qu'une telle conséquence est insoutenable (*untenable*), voir BARAK, p. 17.

725 DUBEY, § 3, N 145.

726 DUBEY, § 3, N 145.

La seule exception à ce principe unanimement admise figure à l'art. 8 al. 3 3ème phrase Cst. : toute personne qui prétend être victime d'une discrimination salariale en raison de son sexe peut invoquer cette disposition constitutionnelle envers un autre particulier. En d'autres termes, cette disposition constitutionnelle peut déployer un effet horizontal direct. Quant à savoir si d'autres droits fondamentaux se prêtent à une application directe entre particuliers, la doctrine est partagée[727]. La majorité de la doctrine ne considère toutefois pas que l'art. 13 al. 2 Cst. devrait déployer un tel effet[728].

Toutefois, ces quelques développements n'impliquent aucunement que les droits fondamentaux ne déploient aucun effet entre particuliers. En effet, l'art. 35 al. 1er Cst. prévoit que « les droits fondamentaux doivent être réalisés dans l'ensemble de l'ordre juridique ». La consécration de la fonction dite objective des droits fondamentaux implique que les valeurs véhiculées par les droits fondamentaux doivent être mises en œuvre par l'État dans l'accomplissement de ses tâches et rayonner dans l'ensemble de l'ordre juridique, c'est-à-dire également dans les relations entre particuliers[729]. En effet, dans quelques hypothèses, certains particuliers peuvent porter atteinte aux intérêts individuels fondamentaux que les droits fondamentaux ont pour objet de protéger[730]. Ainsi, l'art. 35 al. 3 Cst. vient préciser l'art. 35 al. 1er Cst. dans les relations entre

727 DUBEY mentionne la liberté d'association positive et négative, la liberté syndicale positive et négative et le droit de grève, voir DUBEY, § 3, N 148 ; MARTENET quant à lui écrit qu'« une évolution vers une horizontalité directe ou quasi directe des art. 10 al. 3 Cst., 15 al. 4 Cst., 17 al. 3 Cst. et 28 al. 3 Cst. notamment ne paraît pas exclue, même si la jurisprudence est soit inexistante soit embryonnaire à cet égard, voire équivoque », voir MARTENET, art. 35 Cst., N 81, avec de multiples références supplémentaires.

728 MEIER, Protection des données, N 24 ; FLÜCKIGER, p. 852 ; *a contrario* DUBEY, § 3, N 146 ss. ; dans le contexte du droit du travail, RUDOLPH considère que deux droits fondamentaux seulement déploient un effet horizontal direct entre employeur et employé (art. 8 al. 3 3ème phrase Cst. et 110 al. 3 Cst.), l'art. 13 al. 2 Cst. ne faisant pas partie de cette courte liste, voir RUDOLPH, Richterliche Rechtsfindung, N 226 ss. ; pour une analyse plus approfondie de cette question, voir *infra* Chapitre 11. Le cadre constitutionnel suisse.

729 DUBEY, § 3, N 149 ss.

730 De manière générale, voir PULVER, p. 414 ou BARAK, p. 16 ; spécifiquement par rapport à une potentielle atteinte à divers droits fondamentaux en raison de la position de force qu'une des parties au contrat de droit privé occupe par rapport à l'autre partie au contrat, voir DUBEY, § 3, N 141 ; spécifiquement par rapport au droit fondamental au respect de la vie privée, voir REHM, Digital Age, p. 378 ; on notera que dans leur article fondateur publié en 1890, WARREN et BRANDEIS craignaient davantage les atteintes au droit au respect de la vie privée commises par des privés trop curieux que par les pouvoirs publics, voir WARREN S./BRANDEIS, p. 195 ; on pensera également à l'exemple cité en guise d'introduction, pour une comparaison entre la surveillance publique et la surveillance privée, voir *supra* Chapitre 1. D'une surveillance publique à une surveillance privée.

particuliers[731] et se lit comme suit : « les autorités veillent à ce que les droits fondamentaux, dans la mesure où ils s'y prêtent, soient aussi réalisés dans les relations qui lient les particuliers entre eux ». Cette réalisation incombe tant aux autorités exécutives qu'aux pouvoirs législatif ou judiciaire[732]. Ainsi, dans certains cas de figure, les autorités doivent activement prendre des mesures afin de protéger les intérêts des individus concernés. En d'autres termes, la Cst. impose, dans certaines hypothèses, des obligations dites positives à l'État (notion développée par le Cour EDH puis reprise par le Tribunal fédéral)[733]. Dans ces hypothèses, les droits fondamentaux vont déployer un effet indirect entre les particuliers, p. ex. par le biais d'une loi fédérale. Par le biais de la LPD (et d'autres lois spéciales), l'effet horizontal indirect de l'art. 13 al. 2 Cst. est reconnu de longue date et ne doit pas faire l'objet de plus amples développements à ce stade[734]. En effet, la LPD régit non seulement les traitements effectués par les organes fédéraux mais aussi ceux effectués par des responsables de traitement privés[735]. La question qui se pose est alors celle de savoir si le Législateur a eu suffisamment égard aux intérêts fondamentaux protégés par l'art. 13 al. 2 Cst., lorsqu'il a adopté respectivement révisé la LPD. Certains l'affirment[736], d'autres sont plus réservés[737]. En d'autres termes, la question est donc celle

731 SCHEFER, p. 1133.

732 PÉTERMANN, pp. 11 s.

733 MARTENET, art. 35 Cst., N 78 s. ; dans le même sens, mais moins explicite, voir WERRO/SCHMIDLIN, p. 184 ; WERRO et SCHMIDLIN relèvent par ailleurs, qu'en 1993, le Tribunal fédéral a admis ce devoir de protection de manière générale, c'est-à-dire en rapport avec chacun des droits fondamentaux, voir idem, p. 183.

734 À titre d'exemple, voir DUBEY, § 3, N 151 ; KIENER, § 30, N 78 ; BIAGGINI, art. 13 al. 2 Cst., N 16.

735 Art. 1er LPD.

736 MEIER, Protection des données, N 24 (par rapport à l'aLPD) ; DUBEY, § 3, N 151 (par rapport à l'aLPD) ; KIENER, § 30, N 78 ; le Conseil fédéral, dans son rapport relatif aux conséquences de la numérisation sur l'emploi et les conditions de travail publié en 2017 semble chercher sa voie : En effet, il estime que « de manière générale, la situation actuelle n'appelle pas de mesures législatives majeures. De l'avis du Conseil fédéral, les dispositions en matière de protection des données [...] sont opérantes, même dans le contexte de la mutation en cours » alors que quelques pages avant il affirme que la nLPD « tient *partiellement* compte des problématiques liées à la numérisation, en introduisant dans la loi le profilage [...], et en prévoyant des devoirs particuliers pour les responsables du traitement qui y recourent. Ces règles seront pertinentes dans le domaine du droit du travail à l'embauche », voir Rapport du Conseil fédéral « Conséquences de la numérisation sur l'emploi et les conditions de travail : opportunités et risques », 8 novembre 2017, pp. 72 et 103.

737 SCHWEIZER R., art. 13 al. 2 Cst., N 43 ; HERTIG RANDALL/MARQUIS, art. 13 al. 2 Cst., N 63 et N 73 ss. ; RUDOLPH, Richterliche Rechtsfindung, N 55.

de savoir si le pouvoir judiciaire[738] devrait constater l'existence d'obligations positives[739] supplémentaires auxquelles le Législateur n'a pas su répondre de manière satisfaisante dans le cadre de la révision.

On notera qu'une approche dogmatique aux conditions qui permettent d'affirmer l'existence d'obligations positives en droit constitutionnel suisse (et dans la jurisprudence de la Cour EDH[740]) fait défaut. Reprenant l'approche en quatre temps proposée par PULVER[741], il convient de déterminer, par la suite, dans quelle mesure l'art. 13 al. 2 Cst. se prête à la consécration d'obligations positives non encore consacrées dans la LPD ou dans la jurisprudence du Tribunal fédéral.

En principe, les obligations positives peuvent découler de n'importe quel droit fondamental[742]. Il convient de noter que les titulaires de droits fondamentaux doivent être protégés non seulement contre les violations de leurs droits, mais aussi contre les risques de telles atteintes à leurs droits. Ainsi, dans un premier temps, on peut se demander si, dans le cas d'espèce, le ou les droits fondamentaux se prêtent à une application entre particuliers et si tel est le cas, s'il a été porté atteinte à un intérêt individuel fondamental qu'un de ces droits a pour objet de protéger (ou si une telle atteinte risque de se produire). Les obligations positives ne seront toutefois uniquement admises lorsqu'il existe

738 Pour une appréciation critique de l'accroissement du rôle du juge en matière de l'interdiction de discriminer sur le lieu du travail (qui vaut *mutatis mutandis* également dans le contexte de cette contribution), voir MARTENET, La protection, pp. 428 et 446 ; on rappellera également que les obligations positives s'adressent, en principe, à toutes les branches de l'État, le juge reste cependant la première autorité concernée par ces obligations, voir BESSON, Humaniser le droit privé, pp. 19 ss.

739 En guise de clarification, on rappellera que les obligations positives telles que conçues par la Cour EDH sont à la charge de l'État, mais leur portée revient « pratiquement à conférer *de facto* un effet horizontal sinon direct du moins quasi direct aux droits fondamentaux concernés », voir, à titre d'exemple, MARTENET, art. 35 Cst., N 86.

740 WERRO/SCHMIDLIN, p. 186.

741 On rappellera que PULVER fonde son approche sur la jurisprudence (casuistique) de la Cour EDH ainsi que sur la thèse d'EGLI soutenue en 2002 et les travaux de LIENHARD, voir, pour de plus amples références, PULVER pp. 416 ss. ; de surcroît, on notera, qu'en général, les libertés individuelles se prêtent mieux à une application (partielle) entre particuliers que les droits sociaux ou politiques, voire les garanties relatives à l'État de droit, voir FASNACHT, N 92 et WERRO/SCHMIDLIN, pp. 180 s. ; pour une affaire qui portait sur l'étendue des obligations positives lors d'une mesure de surveillance mise en place sur le lieu de travail et qui reprend la structure décrite par PULVER, voir Cour EDH [GC], *Barbulescu c. Roumanie*, 5 septembre 2017, n° 61496/08, §§ 69 ss.

742 WERRO/SCHMIDLIN, p. 183 ; MARTENET précise que « la théorie des obligations positives a surtout été développée par la Cour EDH en se fondant sur plusieurs articles de la CEDH [...]. De telles obligations résultent aussi des droits fondamentaux garantis par la Constitution fédérale ; autrement dit, elles ne découlent pas de l'art. 35 al. 3 Cst., mais des droits concernés », voir MARTENET, art. 35 Cst., N 78.

une probabilité non-négligeable qu'une telle atteinte aura lieu, notamment si les événements suivent leur cours habituel ou que les conséquences négatives en cas d'atteinte seraient particulièrement graves[743].

Dans un deuxième temps, il convient de rechercher si une quelconque mesure étatique serait en effet apte à prévenir l'atteinte ou à réduire le risque d'atteinte au droit fondamental en question. En d'autres termes, il sied de déterminer si une des mesures étatiques à disposition des autorités aurait permis de protéger les droits des particuliers de manière adéquate[744].

Si les particuliers se prévalent de leurs droits fondamentaux dans un rapport de droit privé, ils sont souvent les deux à pouvoir opposer (à l'autre) un droit fondamental. Cette possibilité génère des conflits de droits fondamentaux. Ainsi, le juge est appelé à procéder à une pesée des intérêts dans le cas d'espèce[745]. Ce faisant, le juge devra prendre en compte la gravité de l'atteinte et l'importance des droits invoqués dans le contexte précis. À juste titre, PULVER souligne que plus l'une des deux parties au rapport privé est anonyme, puissante et du fait de sa structure ressemble à une autorité publique, plus le respect des droits fondamentaux de l'autre partie au rapport peut lui être imposé[746]. De surcroît, on rappellera que certains intérêts publics prépondérants peuvent également limiter les obligations positives qui incombent à l'État.

Les organes de l'État, et en particulier le Législateur, disposent d'une importante marge d'appréciation lorsqu'ils sont appelés à choisir les mesures qu'ils souhaitent mettre en place[747]. Dans ce contexte, il convient de prendre en considération les moyens limités de l'État, y compris ses moyens financiers limités[748], et le principe de proportionnalité[749]. Toutefois, si la marge d'appréciation des organes étatiques est importante, elle n'est pas illimitée. Les mesures

743 Pour des réserves allant dans le même sens, voir MARTENET, La protection, p. 435.

744 Si l'analyse porte sur une loi fédérale, on rappellera qu'« en matière de droit privé, l'analyse porte avant tout sur des actes normatifs fédéraux largement immunisés […] par l'article 190 Cst. féd. Les silences qualifiés découlant de tels actes sont aussi immunisés », voir MARTENET, La protection, p. 436.

745 Dans le même sens, voir MARTENET, La protection, p. 427 et WERRO/SCHMIDLIN, pp. 183 s.

746 WERRO et SCHMIDLIN confirment cette analyse de PULVER, voir WERRO/SCHMIDLIN, p. 188.

747 Dans le même sens, voir MARTENET, La protection, p. 436 ; pour une analyse critique de cette marge d'appréciation des autorités publiques, des justifications économiques et du test de proportionnalité qu'elle qualifie de « dangers des obligations positives », voir BESSON, Humaniser le droit privé, pp. 30 ss.

748 Dans le même sens, voir WERRO/SCHMIDLIN, p. 183.

749 Pour des précisions quant à la portée du principe de proportionnalité, voir MARTENET, La protection, pp. 439 s.

choisies devront permettre de garantir une protection efficace contre les (potentielles) atteintes aux droits fondamentaux des particuliers. Le choix des mesures devra donc s'opérer à la lumière du critère de l'efficacité.

Une violation d'une obligation positive devrait ainsi uniquement être admise lors d'atteintes d'une certaine gravité ou dans les hypothèses d'inaction manifeste de la part des autorités. En effet, la consécration d'une obligation positive présuppose une violation d'un droit fondamental par un tiers d'une telle gravité à ce que la pesée des intérêts en cause rende la prise de mesures nécessaire et que ces mesures, qui font défaut, étaient raisonnablement exigibles[750].

Tout comme les conditions qui permettent de déterminer l'existence ou non d'obligations positives, l'analyse des conséquences juridiques qui devraient découler de ces obligations positives n'a pas non plus été effectuée en détail en droit suisse. Ainsi, PULVER précise, qu'en principe, toutes les conséquences juridiques, qui peuvent être appliquées après une violation d'un droit avérée, doivent être prises en considération[751]. Lorsqu'une violation d'une obligation positive est dénoncée, il ne s'agit pas de faire constater une action étatique, mais plutôt de faire valoir une inaction d'un ou plusieurs organes de l'État. Ainsi, l'annulation ou la non-application d'une norme ou d'une décision ne semblent pas constituer des mesures aptes à procéder à un rétablissement en l'état. Afin de garantir une protection efficace des droits fondamentaux des particuliers entre eux, d'autres mesures paraissent en effet plus appropriées.

Les arrêts de la Cour EDH ont valeur déclaratoire en ce qu'ils constatent la violation d'obligations positives sans pour autant être directement applicable en droit interne. En effet, les Hautes parties contractantes sont tenues de respecter les arrêts de la Cour EDH[752] et de les implémenter en droit interne. Comme en droit de la CEDH, la constatation d'une violation d'une obligation positive peut ainsi être accompagnée de directives quant à une nouvelle réglementation et ainsi encourager le dialogue entre le pouvoir judiciaire et le pouvoir législatif.

La constatation d'une telle violation peut également imposer l'interprétation des normes existantes à la lumière des droits fondamentaux. Ces interprétations sont importantes en pratique, notamment lorsque le juge est appelé à

750 PULVER, p. 417 ; dans ce contexte, MARTENET précise qu'il convient d'accorder un délai raisonnable au Législateur, voir MARTENET, La protection, pp. 437 s.

751 PULVER, pp. 417 ss. ; pour une énumération de possibles conséquences allant dans le même sens, voir MARTENET, art. 35 Cst., N 79 s. ; pour des exemples similaires ainsi que certains exemples allant plus loin, voir BESSON, Humaniser le droit privé, p. 20.

752 Art. 46 al. 1er CEDH.

concrétiser certaines normes assez vagues comme p. ex. en matière de droit du travail[753]. On retrouve ici l'interprétation qui est communément connue sous la notion malencontreuse[754] d'« effet horizontal indirect »[755].

Constater la violation d'une obligation positive peut conduire le pouvoir judiciaire à combler une carence de l'ordre juridique. Une telle démarche peut ressembler à une application directe des droits fondamentaux entre privés[756]. Au nom de la sécurité juridique, cette conséquence devrait toutefois rester exceptionnelle[757].

En sus de constater une violation de la CEDH, la Cour EDH peut ordonner le versement d'une satisfaction équitable[758]. De telles compensations sont en effet versées lorsque le Législateur ou les autorités d'exécution ne respectent pas leurs obligations positives. En droit interne, il existe également une possibilité d'octroyer des compensations financières, notamment sur le fondement

753 RUDOLPH, Richterliche Rechtsfindung, N 229.

754 KIENER précise que « [traduction] pour cet effet, on utilise parfois le terme d'effet horizontal indirect. Cette notion est cependant ambiguë dans la mesure où il ne s'agit pas d'un effet des droits fondamentaux entre particuliers, mais de l'*obligation de l'État* (sic) de contribuer à la réalisation de l'idée des droits fondamentaux également dans les relations entre particuliers », voir KIENER, § 30, N 77.

755 DUBEY décrit cet effet comme suit : « dans ce contexte [...], l'État doit œuvrer à la réalisation des droits fondamentaux, quand bien même ces derniers ne peuvent pas s'en prévaloir directement contre lui, pour en obtenir le respect. Cela, qu'il s'agisse d'adopter les règles régissant les rapports entre particuliers (fonction législative) ou de leur appliquer ces règles (fonction judiciaire) », voir, pour de plus amples développements, DUBEY, § 3, N 149 ss. ; pour des développements allant dans le même sens, on consultera MARTENET qui précise à ce sujet que « le TF admet d'ailleurs, à juste titre, de retenir une interprétation [d'une norme qui recèle un potentiel d'interprétation] allant à l'encontre du texte de la disposition légale s'il ne reproduit pas son sens véritable, surtout si celui-ci apparaît plus conforme à la Constitution que son texte », voir MARTENET, art. 35 Cst., N 87 ss., et avant tout N 88.

756 À juste titre, MARTENET précise qu'« en se référant à un droit fondamental pour combler une lacune [...], le TF ne reconnaît pas, dogmatiquement parlant, un effet horizontal direct à ce droit, mais reste dans le cadre du droit ordinaire en agissant, le cas échéant, *modo legislatoris*. En se fondant sur des différents critères d'interprétation des droits fondamentaux, le TF peut selon nous faire un pas supplémentaire et arriver à la conclusion que telle ou telle composante d'un droit fondamental produit un véritable effet horizontal direct », voir MARTENET, art. 35 Cst., N 82 s. ; pour plus de précisions quant à cette distinction entre l'effet direct et ce que MARTENET appelle l'« effet prétorien », voir MARTENET, La protection, pp. 445.

757 Dans le but d'améliorer la sécurité juridique, MARTENET estime que le juge, qui constate la nécessité de réaliser un droit fondamental entre particuliers, devrait l'annoncer, p. ex. dans le cadre d'un *obiter dictum*. Lorsque cette nécessité est très largement admise, p. ex. parce qu'elle est prévue dans un traité international liant la Suisse (on pensera, p. ex. à la Convention 108+), un tel avertissement ne serait pas nécessaire, voir, pour plus de détails, MARTENET, La protection, pp. 440 ss.

758 Art. 41 CEDH.

de la responsabilité de l'État. Une telle compensation est également concevable lorsque l'État n'a pas respecté une obligation positive. Cette dernière mesure ne nous intéressera pas davantage dans le cadre de cette contribution.

Sur la base du schéma ainsi esquissé, il convient de déterminer si et dans quelle mesure des obligations positives découlent de l'art. 13 al. 2 Cst., notamment lorsqu'un profilage est effectué pendant une procédure d'embauche.

C. Les obligations positives lors d'un profilage effectué lors de l'embauche

Afin de déterminer les contours de la protection constitutionnelle offerte par l'art. 13 al. 2 Cst. dans le cas particulier d'un profilage effectué dans le cadre d'une procédure d'embauche, il convient de circonscrire dans quelle mesure certaines obligations positives découlent de cette disposition (1) avant d'analyser les potentielles conséquences juridiques de ces obligations positives (2).

1. La constatation de l'existence d'une obligation positive

A titre préliminaire, il convient de relever que plusieurs obligations positives ont déjà pu être consacrées sur le fondement de l'art. 13 al. 2 Cst. On pensera notamment à l'obligation des autorités compétentes de garantir le droit d'accès, le droit de corriger les données personnelles erronées ou encore le droit d'effacer les données personnelles traitées de manière illicite[759]. Cela étant, la première question qui se pose dans le cadre de cette troisième partie est celle de savoir si le profilage effectué pendant une procédure d'embauche porte atteinte ou risque de porter atteinte au droit à l'autodétermination en matière informationnelle[760]. On se souviendra que le droit à l'autodétermination en matière informationnelle peut être décrit comme « le droit à ne pas accepter un traitement qui ne correspond pas à la volonté exprimée [de la personne concernée] »[761], voire « garantit [...] que l'individu demeure maître de ses données personnelles »[762]. Comme nous l'avons vu plus haut, le profilage implique une importante perte de contrôle non seulement sur les données personnelles

759 À titre d'exemple, voir FASNACHT, N 154 ss.

760 Comme mentionné dans le cadre de l'introduction, l'atteinte potentielle à d'autres droits fondamentaux ne fait expressément pas partie de cette analyse, voir *supra* Méthodologie.

761 MEIER, Protection des données, N 17 ; pour une analyse plus extensive de la genèse de ce droit, qui ne figure pas dans la Cst., voir *supra* Chapitre 11. Le cadre constitutionnel suisse.

762 HERTIG RANDALL/MARQUIS, art. 13 Cst., N 62 ; FLÜCKIGER décrit une idée similaire en précisant que « le droit à l'autodétermination en matière de données personnelles [...] garantit à chacun le droit de décider de la diffusion et de l'utilisation de ses données personnelles », voir FLÜCKIGER, p. 837.

(et potentiellement non-personnelles), mais aussi sur les (nouvelles) informations qui peuvent être déduites de ces données. En effet, ces évaluations s'effectuent le plus souvent à l'insu des personnes concernées et, de surcroît, sur la base d'opérations algorithmiques et donc *a fortiori* incontrôlables[763]. Une atteinte à ce droit fondamental doit donc être admise.

Ensuite, il convient de déterminer si les autorités auraient eu la possibilité d'adopter des mesures aptes à éviter l'atteinte. Dans ce cadre, plusieurs potentielles mesures méritent d'être mentionnées. Dans une veine très générale, le Législateur aurait pu améliorer la sécurité juridique en renonçant à la définition problématique du « profilage à risque élevé », augmenter la protection des droits des personnes concernées en prévoyant un droit d'accès renforcé lors d'un profilage, étendre les compétences des autorités de surveillance afin de garantir un recours effectif en cas d'atteinte aux droits protégés par la LPD, voire prévoir, outre une définition, un véritable régime plus protecteur lorsqu'un responsable du traitement effectue un profilage. Dans une veine plus précise, le Législateur aurait également pu opter pour des réglementations sectorielles en matière de droit du travail s'inspirant de ce qu'il avait décidé en 1988, voire ce qui a été proposé par le groupe d'accompagnement Révision LPD en 2014[764] ou le groupe d'experts « Avenir du traitement et de la sécurité des données » en 2018[765] ou comme cela a été envisagé en Allemagne peu avant le début des travaux relatifs au RGPD[766]. En outre, s'inspirant des travaux du Conseil de l'Europe[767], le Législateur suisse aurait même pu jouer un rôle précurseur en consacrant un régime nuancé en matière de profilage.

763 Voir *supra* Chapitre 5. Avantages et risques.

764 Rapport du groupe d'accompagnement Révision LPD du 29 octobre 2014, pt. 4.4.6 ; pour une analyse plus détaillée de ce rapport, voir *supra* Chapitre 8. La Loi sur la protection des données.

765 Rapport du groupe d'experts concernant le traitement et la sécurité des données du 17 août 2018, pt. 5.3.1.6 (quant à la nécessité de légiférer en matière de profilage en général) et pt. 5.3.1.9 (quant à la nécessité de légiférer en matière de profilage sur le lieu de travail) ; pour une analyse plus détaillée de ce rapport, voir *supra* Chapitre 8. La Loi sur la protection des données.

766 PRANTL rappelle qu'« [traduction] en 2012/2013, il existait déjà un projet de loi sur la protection des données des travailleurs, mais ces travaux ont été interrompus, notamment en raison du projet de RGPD [au niveau européen]. Celui-ci est désormais [entré en vigueur], mais ne contient malheureusement aucune disposition relative à la protection des données des employés. Cela signifie que le Législateur national est à nouveau sollicité », voir PRANTL, p. 347.

767 On pensera notamment à la Recommandation profilage 2021 et à la Recommandation emploi ; pour une analyse plus approfondie de ce cadre (non-contraignant) proposé par le Comité des Ministres en 2010 (puis révisé en 2021) et 2015 respectivement, voir *infra* Chapitre 12. Le cadre prévu par le Conseil de l'Europe.

Ces quelques exemples non-exhaustifs sont la preuve que le Législateur avait connaissance de la nécessité de légiférer en la matière et aurait eu la possibilité d'adopter des règles offrant un meilleur encadrement du profilage pendant la procédure d'embauche. Dans ce contexte, on rappellera avant tout que le Conseil fédéral estimait, en 2017 déjà, que sur le lieu de travail, le profilage serait avant tout utilisé lors des procédures de recrutement et constatait que le projet de loi n'encadrait cette nouvelle forme de traitement que de manière partielle[768].

Dans un troisième temps, les intérêts des différentes parties doivent être examinés dans le cadre d'une pesée des intérêts. Au-delà du lien de subordination qui caractérise la relation de travail et qui se manifeste déjà pendant la procédure d'embauche, plusieurs droits fondamentaux du candidat peuvent être violés lors d'un profilage. Bien évidemment, on pensera au droit à l'autodétermination en matière informationnelle. En fonction des données traitées et du degré de précision de l'évaluation automatisée, le profilage peut également porter atteinte à la dignité, à l'interdiction de discrimination, au droit à la liberté personnelle (entendu plus largement que le droit à l'autodétermination en matière informationnelle), à la protection de la sphère privée, à la liberté de conscience et de croyance, aux libertés d'opinion et d'information, à la liberté d'association ou encore à la liberté syndicale du candidat. De plus, une restriction de l'utilisation du profilage porte atteinte à la liberté contractuelle de l'employeur et potentiellement à sa liberté économique et à sa liberté d'information. Dans la mesure où il n'est pas encore avéré que les différentes formes d'évaluations automatisées permettent effectivement de choisir les meilleurs candidats, il est tout sauf certain que le profilage d'un candidat permette à l'employeur de profiter d'un avantage concurrentiel en procédant à un tel traitement de données. En sus de cette incertitude, qui relativise l'atteinte aux intérêts de l'employeur, la pesée des intérêts doit tenir compte du lien de subordination et des multiples droits fondamentaux du candidat potentiellement violés[769]. Il découle de ces quelques développements qu'une situation dans laquelle les intérêts de l'employeur primeraient sur ceux des candidats n'est que difficilement concevable.

768 On rappellera que le Conseil fédéral affirmait, en 2017 déjà, que la nLPD « tient *partiellement* compte des problématiques liées à la numérisation, en introduisant dans la loi le profilage […], et en prévoyant des devoirs particuliers pour les responsables du traitement qui y recourent. Ces règles seront pertinentes dans le domaine du droit du travail à l'embauche », voir Rapport du Conseil fédéral « Conséquences de la numérisation sur l'emploi et les conditions de travail : opportunités et risques », 8 novembre 2017, p. 72. En d'autres termes, il était conscient que même le projet de loi ne parvenait pas à encadrer cette nouvelle forme de traitement de données de manière satisfaisante, quand bien même il arrive à une autre conclusion finale, voir idem, p. 103.

769 PULVER, p. 416.

Dans un quatrième et dernier temps, il faut vérifier si les mesures prévues par les autorités permettent de garantir une protection efficace du droit à l'autodétermination en matière informationnelle. En effet, la doctrine semble unanime quant à affirmer que plusieurs prérogatives découlent de l'art. 13 al. 2 Cst. Les développements figurant dans la deuxième partie de cette contribution sont la preuve que les diverses lois potentiellement applicables au stade de la procédure d'embauche ne garantissent pas une protection efficace des intérêts des candidats que leur droit à l'autodétermination en matière informationnelle a pourtant vocation à protéger. Ainsi, notre analyse semble indiquer que l'art. 13 al. 2 Cst. impose plusieurs obligations positives aux différents organes de l'État auxquelles ces derniers n'ont toutefois pas su répondre de manière satisfaisante. En d'autres termes, un profilage effectué pendant une procédure d'embauche peut constituer une violation de cette disposition constitutionnelle. Encore faut-il se pencher sur les possibles conséquences juridiques d'une telle constatation[770].

2. Les possibles conséquences d'une violation d'une obligation positive

D'abord, le pouvoir judiciaire pourrait, à l'image de la Cour EDH, constater l'existence d'une obligation positive dans le cadre de l'accès au marché du travail et adresser des instructions quant à des modifications légales au pouvoir législatif (a) ou se contenter d'interpréter les notions vagues à la lumière de l'art. 13 al. 2 Cst. (b). Enfin, le pouvoir judiciaire pourrait même décider d'adopter une règle par substitution et ainsi reconnaître un effet horizontal direct (partiel) à cette disposition constitutionnelle[771] (c).

a. Les modifications législatives envisageables

(i) Une précision de l'art. 328b CO

La constatation selon laquelle toute relation de travail implique le traitement de données personnelles d'une quantité et d'une variété considérables reste d'actualité, voire est encore plus pertinente aujourd'hui qu'en 1988 lors de

770 Dans une veine similaire, RUDOLPH précise qu'« [traduction] en ce qui concerne les questions juridiques qui se posent dans le contexte de la numérisation [du lieu de travail], force est de constater un vide juridique non négligeable (*faktisch muss von einem nicht unerheblichen gesetzlichen Regelungsvakuum gesprochen werden*). Il faut donc s'attendre à ce que, même et surtout dans le domaine de la numérisation, ce soient les tribunaux, qui posent les jalons et auxquels il revient, ce faisant, de jouer un rôle pionnier en la matière. Ainsi, la force créatrice du droit du travail continuera à se déplacer de la loi vers le droit prétorien », voir RUDOLPH, Richterliche Rechtsfindung, N 55.

771 MARTENET, art. 35 Cst., N 82 s.

l'introduction de l'art. 328b CO[772]. Avec l'introduction de nouvelles définitions légales qui peuvent expressément trouver application dans les relations de travail[773], il est regrettable qu'aucune réflexion n'ait été menée dans le cadre de la révision totale de la LPD quant à une éventuelle précision de l'art. 328b CO[774]. Comme nous l'avons vu plus haut[775], le seul critère de l'évaluation de l'aptitude du candidat fixé par cette disposition et l'application subsidiaire des principes généraux prévus dans la LPD ne sont plus à même de protéger la personnalité des candidats de manière efficace.

Une précision du régime applicable aurait pu inclure une restriction des catégories de données qui peuvent être traitées par l'employeur. Le premier réflexe consiste à vouloir interdire les traitements de données sensibles dans le cadre d'une procédure d'embauche ou du moins de les limiter d'une manière ou d'une autre. Or, comme ROUVROY l'explique grâce à de nombreux exemples, les évaluations effectuées dans le cadre d'un profilage permettent de potentiellement aboutir à des informations sensibles sur la base d'une évaluation de

772 À titre d'exemple, voir PRANTL, p. 347. S'il est vrai que PRANTL cite des exemples de mesures de surveillance mises en place par divers employeurs allemands, la situation en Suisse ne devrait pas différer de manière significative de celle décrite par cet auteur – bien au contraire. En effet, le cadre légal suisse est moins strict que le cadre légal allemand (tant avant qu'après l'entrée en vigueur du RGPD), voir MORGENROTH, pp. 116 s.

773 L'art. 5 let. f LPD fixe expressément que le profilage doit être entendu comme « toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail ».

774 FF 1988 494 ; le Message du Conseil fédéral de 2017 reste complètement muet par rapport aux traitements de données effectués par les employeurs. Dans de termes très vagues, le Conseil fédéral se contente de noter que les « besoins de réforme supplémentaires [tel que suggérés par le groupe d'experts mis en place par le DFF], s'ils devaient être avérés, pourraient être pris en compte lors d'une étape ultérieure. Il n'est d'ailleurs pas exclu que ces besoins de réforme concernent d'autres domaines que la protection des données (p. ex. le code des obligations) ». La seule règle sectorielle qui est discutée, mais qui n'a finalement pas été retenue porte sur une éventuelle interdiction des fichiers de solvabilité, voir FF 2017 6581 s. ainsi que FF 2017 6605 ; une approche sectorielle aurait également été en ligne avec les objectifs de la modernisation de la Convention 108. En effet, les travaux de modernisation avaient, entre autres, pour objectif de « maintenir la nature générale et technologiquement neutre des dispositions de la convention quitte à compléter l'instrument par des textes sectoriels plus détaillés », voir WALTER, Modernisation, p. 4 ; au vu des développements techniques, le Législateur allemand avait songé de prévoir un régime plus strict des traitements de données qui pouvaient être effectués par l'employeur, notamment en adoptant une loi spéciale sur la protection des données des employés (*Arbeitnehmerdatenschutzgesetz*). En raison des travaux relatifs au RGPD, ce projet a été abandonné. Malheureusement, le RGPD ne contient aucune disposition venant protéger les employés, voir PRANTL, p. 347 s.

775 Voir *supra* Chapitre 7. Le Code des obligations.

données non-sensibles[776] voire de données anonymes[777]. Ainsi, une telle interdiction, voire une limitation des catégories de données qui peuvent être traitées ne permettrait pas d'améliorer la protection des droits des candidats. Au vu des difficultés de limiter juridiquement (et techniquement) les traitements à certaines catégories de données, on peut se demander s'il ne serait pas plus opportun de prévoir une interdiction générale du profilage dans le CO[778]. Mesure radicale intéressante à première vue, elle soulève toutefois de nombreux problèmes elle aussi. Une telle interdiction risquerait de constituer une limite excessive à la liberté contractuelle. Par ailleurs, une interdiction exclurait toute utilisation potentiellement bénéfique du profilage. De surcroît, au vu des définitions peu précises du profilage d'une part et du profilage à risque élevé d'autre part, ainsi que de la diversité des profilages possibles, une interdiction du profilage en l'état actuel de la législation risquerait d'être trop générale. On rappellera que même si une telle interdiction était consacrée dans le CO, la mise en pratique de cette interdiction relèverait de l'utopie, notamment au vu de la taille importante du secteur à surveiller et des capacités restreintes du PFPDT.

Ensuite, en vertu du principe de transparence, il convient d'analyser à quel point les droits des candidats pourraient être renforcés s'il existait une obligation explicite[779] de préciser, p. ex. dans les offres d'emploi, que certaines évaluations automatisées vont être effectuées si la personne décide de postuler[780]. Dans ce

776 ROUVROY, p. 27 ; dans le même sens, voir MEIER, Big Data, pp. 58 s.

777 ROUVROY, pp. 20 ss.

778 À propos du droit au logement et au travail, le Comité des Ministres précise qu'« au vu des risques induits, les traitements de données ayant recours au profilage doivent être […] purement et simplement interdits ou soumis à des conditions particulières. En effet, même si, en général, l'on peut admettre que la personne concernée puisse exercer un droit d'accès ou d'opposition par rapport à l'utilisation du profilage dans des traitements peu sensibles, on ne peut pas conditionner l'accès à des biens et services fondamentaux, comme le droit au logement et au travail, au seul résultat – parfois erroné – […] d'un profilage », voir Exposé des motifs, pt. 58.

779 Le devoir d'informer le candidat a été étendu à la collecte de *toutes* les données personnelles et est désormais fixé aux art. 19 à 21 al. 1er et 3 LPD (sous le régime de l'aLPD, le responsable du traitement ne devait qu'informer la personne concernée lors d'une collecte de données *sensibles* ou de profils de la personnalité, voir l'art. 14 aLPD). Toutefois, il n'est pas certain si l'employeur pourrait éventuellement faire valoir une des exceptions au devoir d'informer fixées à l'art. 20 LPD. La consécration d'une obligation explicite aurait le mérite d'améliorer la sécurité juridique. Pour une proposition allant dans le même sens, mais qui ne serait pas limitée aux seuls traitements effectués sur le lieu de travail, mais qui s'appliquerait de manière générale à tous les traitements effectués grâce à des méthodes de *Big Data*, voir ROUVROY, p. 30.

780 Vraisemblablement, certaines entreprises qui offrent de telles évaluations insistent sur le fait que les employeurs rendent le recours à de tels traitements de données transparents, voir Reatch, Wenn Künstliche [sic] Intelligenz über Bewerber*innen

contexte, certains proposent de travailler avec des émoticônes standardisés[781]. Une telle transparence accrue aurait entre autres pour conséquence que le nombre de candidats conscients de telles évaluations augmenterait et que potentiellement plus de demandes d'accès soient enregistrées. De plus, une telle obligation aurait potentiellement pour conséquence que certains employeurs renoncent à ces traitements de données et cherchent à se démarquer d'autres employeurs moins sensibles à la protection des données des candidats. Toutefois, on rappellera les réserves émises plus haut déjà quant à une extension trop importante du principe de transparence[782].

En ce qui concerne le droit d'accès, on peut se demander s'il devrait être précisé lorsque le traitement de données impacte l'accès au marché du travail. À la lumière du droit d'accès, qui découle directement de l'art. 13 al. 2 Cst.[783], le CO aurait pu être complété dans la mesure où le droit d'accéder à l'évaluation n'est pas suffisant[784], notamment si le candidat souhaite faire valoir ses divers droits. Encore faudrait-il que l'employeur soit en mesure d'expliquer l'évaluation faite (ce qui ne sera très probablement pas possible). Ainsi, à défaut d'être en mesure de contextualiser l'évaluation, l'employeur devrait être tenu de procéder à l'évaluation lui-même et expliquer pourquoi le traitement de données effectué n'est pas abusif. Une telle modification reviendrait à renverser le fardeau de la preuve[785]. Dans ce contexte, on rappellera que bien souvent, ce n'est qu'une fois les données imprimées sur une feuille que les personnes concernées se rendent compte des traitements effectués. Reprenant les mots du sociologue STARK, les *data broker* « [traduction] tirent parti d'un phénomène émotionnel simple : nous ne pouvons pas ressentir les données. C'est pourquoi le fait de voir

entscheidet, reprenant les positions défendues lors de la conférence intitulée « Künstliche Intelligenz meets HR : Chancen und Risiken für Arbeitnehmer*innen » organisée à l'Université de Zurich le 29 septembre 2021.

781 CHRISTL/SPIEKERMANN, p. 143.

782 AlgorithmWatch, p. 32 ; voir, pour plus de développements quant à ce principe, *supra* Chapitre 8. La Loi sur la protection des données.

783 SCHWEIZER, art. 13 al. 2 Cst, N 85 ; FLÜCKIGER, p. 852.

784 L'art. 25 al. 2 let. f LPD ne garantit l'accès à la logique qui sous-tend un traitement automatisé uniquement dans les cas d'une décision individuelle automatisée et non dans les cas d'un profilage, qu'il s'agisse d'un profilage « général » ou d'un profilage à risque élevé.

785 Pour un renforcement du droit d'accès, notamment dans l'hypothèse d'un profilage et la consécration d'un renversement (généralisé) du fardeau de la preuve, voir WALTER, Perspectives, N 19 et 23 ; par rapport aux potentiels bénéfices d'un renversement du fardeau de la preuve dans le contexte plus général des traitements de données fondés sur le *Big Data*, voir ROUVROY, p. 34 ; dans ce contexte, rappelons que le PFPDT aurait souhaité la consécration d'un renversement généralisé du fardeau de la preuve dans la nLPD, voir FF 2017 6606.

tout imprimé nous frappe. Nous sommes des créatures physiques. Nous avons besoin de matérialité »[786]. Ainsi, le renforcement du droit d'accès aurait également pour effet d'améliorer la sensibilisation des personnes concernées.

Indépendamment de toute mesure législative concrète, il convient de noter que dans le but d'améliorer la sécurité juridique ainsi que la protection des droits des candidats concernés[787], il est essentiel de ne pas rendre cette matière juridique encore plus touffue.

(ii) Une nouvelle définition de la donnée personnelle sensible

Le droit fondamental à l'autodétermination en matière informationnelle ainsi que la LPD reflètent l'idée selon laquelle la collecte de données personnelles s'opère au moment où la personne concernée met à disposition, avec un degré minimal de prise de conscience et dans un contexte déterminé, ses données personnelles. En d'autres termes, l'art. 13 al. 2 Cst. et la LPD supposent que lorsqu'une personne partage ses données personnelles, elle perd une partie de son contrôle sur lesdites données, mais pas tout son contrôle[788]. Or, force est de constater que les données personnelles mises à disposition directement par les personnes concernées (*individually provided data*) ne représentent plus la source la plus importante de nouvelles données. En effet, comme le mentionnait le WEF dans un rapport publié en 2014 déjà, deux autres sources de données personnelles deviennent de plus en plus importantes. D'une part, il existe de plus en plus de « données observées » (*observed data*), comme p. ex. les préférences de navigation sur Internet, les images enregistrées par une caméra de vidéosurveillance ou les points GPS. D'autre part, il existe de plus en plus de « données déduites » (*inferred data*), comme p. ex. les évaluations proposées à la suite d'un profilage tels les scores de crédit, les profils de consommateurs, la publicité ciblée ou les schémas de propagation de maladies infectieuses[789].

786 Si STARK est cité dans un article relatif à l'application *Tinder*, ses observations valent *mutatis mutandis* par rapport à toute entité privée qui collecte puis évalue des données, voir DUPORTAIL, I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets.

787 CHRISTL et SPIEKERMANN relèvent, à juste titre, qu'en raison de ses multiples renvois internes, le RGPD ne peut plus être mis en œuvre par des juristes non-spécialistes (contrairement à la Directive 95/46/CE). Ainsi, ces auteurs estiment que les juristes spécialisés en protection des données seront mandatés par les entreprises qui peuvent se permettre de les rémunérer. La complexité de la matière aura pour conséquence à long terme que les spécialistes proposent une interprétation du RGPD bénéfique aux intérêts de leurs clients, allant ainsi à l'encontre des intérêts des personnes concernées, voir CHRISTL/SPIEKERMANN, p. 141.

788 FLÜCKIGER, pp. 837 s. et, dans une veine plus internationale, voir WEF, p. 16.

789 WEF, pp. 16 s. On notera que cette catégorisation des données traitées proposée par le WEF correspond aux trois étapes du processus du profilage tel que décrit par le Comité des Ministres, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 38.

Au vu de ces développements, on peut légitimement se demander si la notion de « donnée personnelle sensible » doit être réévaluée, notamment lors d'un profilage. En effet, si la liste des données sensibles a été élargie dans le cadre de la révision, cette liste est exhaustive. Dans ce contexte, on rappellera que le traitement de données personnelles sensibles entraîne l'application d'un régime de protection plus strict[790].

Prévoir différents régimes en fonction du risque posé par le traitement envisagé semble justifié dans la mesure où les traitements de données qui ne soulèvent aucun risque pour les droits et libertés des personnes concernées sont nombreux. Toutefois, au regard des développements décrits ci-dessus, il semble qu'un régime plus strict applicable en fonction de la nature de la donnée plutôt qu'en fonction du processus de traitement ne soit plus en ligne avec les nouvelles formes de traitements et leurs potentiels impacts sur les droits et libertés des personnes concernées. Ainsi, afin de tenir compte de ces développements, la réévaluation de la notion de « donnée sensible » impliquerait d'abandonner, du moins en partie, l'idée selon laquelle la personne concernée peut maintenir le contrôle sur ses données et de rechercher plus précisément si la forme de traitement porte (ou non) atteinte à la dignité et à l'identité de la personne concernée (qui sont également protégées par l'art. 13 al. 2 Cst.[791]). S'il s'agit d'une « donnée déduite », le régime plus protecteur des droits et libertés devrait alors, en principe, trouver application, même si le traitement ne porte pas sur des données sensibles. Le profilage est un traitement qui tombe dans cette catégorie. Si soumettre le profilage au régime plus protecteur de la LPD aurait, par ailleurs, été en ligne avec la volonté initiale du Législateur[792], la consécration d'un tel régime aurait toutefois eu pour conséquence de soumettre même les profilages peu problématiques à un régime renforcé.

Dans le cadre des travaux de modernisation de la Convention 108, le comité consultatif a essayé de trouver un compromis, en qualifiant de donnée sensible « les données qui, du fait de leur traitement présentent un risque grave pour les intérêts, les droits et les libertés fondamentales de la personne concernée, notamment un risque de discrimination [...]. Cette proposition permettait de

790 Art. 6 al. 7 let. a LPD ; art. 22 al. 2 let. a LPD ; art. 30 al. 2 let. c LPD ; art. 31 al. 2 let. c ch. 1 et let. e ch. 2 LPD.

791 DIGGELMANN, art. 13 Cst., N 7.

792 FF 2017 6677 ; notons qu'en droit européen, un profilage qui n'est pas suivi d'une décision individuelle automatisée n'est pas spécifiquement encadré par la partie contraignante du RGPD. Toutefois, le cons. 71 par. 2 encourage les responsables du traitement à mettre en place certaines mesures afin de garantir un profilage « équitable ». Ces mesures devraient, entre autres, tenir compte des circonstances particulières et du contexte du profilage effectué.

considérer certains traitements comme sensibles, non seulement sur la base de la nature des données, mais également en tenant compte de la finalité et des circonstances de traitement »[793]. Cette définition a toutefois été rejetée, car jugée trop floue[794].

(iii) L'indépendance du PFPDT renforcée et l'octroi de compétences supplémentaires

Plusieurs mesures mises à disposition des autorités de surveillance européennes, mais inconnues en droit suisse, ont eu un impact significatif en pratique. On pensera notamment à la possibilité laissée aux autorités de surveillance d'engager une procédure au nom et pour le compte d'une personne concernée[795] ou d'infliger des sanctions administratives[796] forçant les responsables à aborder les questions de protection des donnés dans le cadre des débats stratégiques de leurs entreprises.

S'inspirant du droit de la protection des données de l'UE, l'octroi de compétences plus importantes au PFPDT serait un moyen envisageable afin de garantir une mise en œuvre plus efficace du droit de la protection des données[797] et constitue, de surcroît, un « élément central pour la reconnaissance de l'adéquation de la législation suisse »[798] par l'UE. On notera toutefois que l'octroi de compétences supplémentaires n'améliorera la protection des droits des candidats qu'à condition que l'autorité de surveillance puisse prendre ses décisions en toute indépendance et en temps utile, notamment grâce à des ressources personnelles suffisantes[799]. Or, si la révision a apporté quelques améliorations quant à l'indépendance du PFPDT et que le Conseil fédéral a approuvé

793 WALTER, Modernisation, p. 11.

794 WALTER, Modernisation, p. 11.

795 Art. 58 RGPD.

796 Art. 83 al. 4-6 RGPD ; pour un bref résumé des raisons qui ont conduit le Conseil fédéral à écarter cette option, voir FÜZESSÉRY/SCHNEIDER, p. 158.

797 WALTER, Perspectives, N 32 ss.

798 FÜZESSÉRY/SCHNEIDER, p. 157 ; MÖHLE, pp. 599 ss.

799 ROSENTHAL va même plus loin puisqu'il estime que la révision de l'aLPD n'aurait pas été nécessaire. Une amélioration de la protection de la personnalité des personnes concernées aurait pu être atteinte en prévoyant des ressources bien plus importantes pour le PFPDT (*dem Datenschutz wäre wesentlich mehr gedient [als eine Revision], wenn dem EDÖB massiv mehr Mittel zur Erfüllung seiner Aufgaben zur Verfügung stehen würden*). Il reconnaît toutefois qu'une telle augmentation des moyens du PFPDT est illusoire d'un point de vue politique, voir ROSENTHAL, Entwurf, N 4 ; dans son rapport actuel, le PFPDT reconnaît lui-même que sa « surveillance ne satisfait que partiellement les attentes justifiées du public », notamment en raison de l'« insuffisance persistante des moyens », PFPDT, 29e Rapport d'activités, p. 10.

la création de postes supplémentaires avec l'entrée en vigueur de la nouvelle LPD[800], certains aspects du fonctionnement de cette autorité de surveillance méritent néanmoins d'être analysés de manière critique.

D'abord, WALTER précise, à juste titre, que la nomination puis l'élection du PFPDT ne devraient pas conduire à trop politiser la fonction[801]. Si le changement opéré dans le cadre de la révision est certes conforme aux exigences européennes[802], il risque toutefois de politiser davantage cette fonction. Contrairement à ce que le Conseil fédéral souhaitait[803], la nouvelle LPD prévoit que le PFPDT n'est plus nommé puis élu par le Conseil fédéral mais par le Parlement[804]. Sa nomination et son élection peuvent alors être influencées par des groupes d'intérêts[805]. Si l'on songe aux 2'000 lobbyistes engagés par les différents groupes d'intérêts européens dans le but d'influer sur le contenu du RGPD[806], la position du Conseil fédéral semble à tout le moins prudente[807]. La pandémie a prouvé que les questions portant sur la protection des données sont arrivées au cœur des débats actuels les plus virulents[808]. Au vu de cette prise de conscience collective et de la modification de la procédure d'élection du PFPDT, il n'est que peu probable que la prochaine élection sera moins politisée que la précédente[809]. Ainsi, la révision ne semble pas avoir apporté l'apaisement

800 PFPDT, Nouvelle LPD : 5 postes supplémentaires à partir de juillet 2022.

801 WALTER, L'indépendance, p. 73.

802 La Convention 108+ ne prévoit pas de disposition concernant le mode d'élection ou de nomination de l'autorité de contrôle. L'art. 53 RGPD oblige les États membres à régler la procédure de nomination, tout en leur laissant le choix entre une nomination par le parlement, le gouvernement, le chef d'État ou encore par un organisme indépendant.

803 FF 2017 6703.

804 Art. 43 al. 1er LPD.

805 FF 2017 6703.

806 CHRISTL/SPIEKERMANN, p. 139.

807 Dans ce contexte, on rappellera que la Suisse ne connaît qu'une législation très rudimentaire en matière de lobbying. En effet, l'accès des lobbyistes ou représentants d'intérêts au Palais du Parlement est uniquement réglementé par l'art. 69 al. 2 de la Loi sur le Parlement (LParl) du 13 décembre 2002, RS 171.10, voir, pour une analyse du cadre légal suisse, FF 2018 7069. Ce Message du Conseil fédéral faisait suite à une initiative parlementaire du conseiller aux États BERBERAT déposée en 2015. Pour les raisons pour lesquelles il a été décidé de ne pas réviser le régime prévu par la LParl en profondeur, voir FF 2018 7659.

808 Dans le contexte de la pandémie, à titre d'exemple, voir DIBBASEY/STUDER, « Airlines können keine Impfausweispflicht einführen »; pour un exemple international, voir MÄDER/FULTERER, Plattform für Menschenhandel, Schäden bei Teenagern, falsche Nutzerzahlen : Das sind die Vorwürfe der Facebook-Whistleblowerin.

809 À titre d'exemple, voir IMBACH, Datenschützer : Massive Kritik am Vorschlag des Bundesrates.

souhaité par WALTER – bien au contraire[810]. Cette constatation est particulièrement regrettable dans la mesure où les réponses données aux questions soulevées sur le lieu de travail risquent d'être influencées par le point de vue politique du PFPDT, voire par les groupes d'intérêts qui auront soutenu sa candidature.

Ensuite, WALTER suggère qu'un autofinancement contribuerait à l'amélioration de l'indépendance du PFPDT[811], dont le projet de budget est remis par l'intermédiaire de la Chancellerie fédérale au Conseil fédéral qui le transmet ensuite tel quel à l'Assemblée fédérale[812]. En vertu de l'art. 59 LPD, introduit dans le cadre de la révision, le PFPDT peut percevoir des émoluments tel que fixés à l'art. 44 OPDo. Dans le but de permettre un accès à ses services à tout un chacun, les émoluments ne sont pas très conséquents (tarif horaire variant entre 150 et 250 francs, selon la fonction exercée par la personne concernée). Même avec l'introduction de cette nouvelle compétence dans le cadre de la révision, les émoluments perçus ne vont donc pas contribuer à une indépendance financière accrue du PFPDT.

Enfin, la liste des incompatibilités a été précisée dans le cadre de la révision. Il est toutefois regrettable que la LPD n'ait pas étendu une liste des incompatibilités aux collaborateurs[813].

(iv) Un régime pénal plus strict

On rappellera dans ce contexte, que pour certains spécialistes, le processus de dé-anonymisation devrait être interdit et sanctionné pénalement[814]. Une telle proposition est compréhensible dans la mesure où il est facile d'imaginer plusieurs constellations dans lesquelles une dé-anonymisation peut porter atteinte à l'honneur, voire au domaine secret ou privé[815]. À l'image de la Cour EDH, le Tribunal fédéral pourrait alors être tenté de constater la violation d'une obligation positive dans le domaine pénal[816]. Toutefois, d'un point de vue pratique, une pénalisation de tout processus de dé-anonymisation, ce qui reviendrait à

810 Dans le même sens critique, avec de plus amples développements, voir MONTAVON, pp. 707 s.

811 WALTER, L'indépendance, p. 74.

812 Art. 45 LPD ; pour une analyse critique (à juste titre) de cette nouveauté introduite lors de la révision, voir MONTAVON, p. 701.

813 Les collaborateurs du PFPDT ne sont que soumis aux exigences de l'art. 20 al. 2 de la Loi sur le personnel de la Confédération (LPers) du 24 mars 2000, RS 172.220.1, qui fixe uniquement que « pendant la durée du contrat, l'employé ne peut exercer pour un tiers une activité rémunérée que dans la mesure où il ne viole pas son devoir de fidélité » ; dans le même sens, voir MONTAVON, p. 704.

814 CHRISTL/SPIEKERMANN, p. 142.

815 Intitulé du Titre 3 du Livre 2 du Code pénal suisse.

816 Cour EDH, *X. et Y. c. Pays-Bas*, 26 mars 1985, n° 8978/80.

une interdiction totale de cette pratique, semble illusoire au vu de la taille de ce secteur économique et de son potentiel développement. De plus, la consécration d'une nouvelle infraction est justifiée si la poursuite de cette infraction peut être assurée par les autorités compétentes. Or, comme nous l'avons vu plus haut, les autorités compétentes en la matière sont les autorités de poursuite cantonales. Ces autorités cantonales n'ont que peu d'expérience quant au volet pénal du droit de la protection des données. Par ailleurs, une compétence cantonale en la matière semble aller à l'encontre d'une application uniforme du droit de la protection des données pourtant essentielle dans un monde économique interconnecté. En outre, il va sans dire que si les autorités pénales suisses ne peuvent pas poursuivre des infractions commises par des courtiers en données qui siègent à l'étranger, elles pourraient poursuivre les infractions commises par les employeurs établis en Suisse. On notera enfin que sous peine de distorsion concurrentielle, une prohibition n'aurait de sens que si elle était décidée pour la planète entière – ce qui relève de l'utopie[817]. Un encadrement plus efficace des traitements de données à grande échelle semble dès lors plutôt passer par une réévaluation (internationale) de l'« économie de la surveillance »[818] que par la consécration d'une interdiction pénale du processus de dé-anonymisation.

817 Au-delà de la difficulté de convaincre tous les pays de consacrer une telle interdiction, MEIER cite les réserves émises par OHM, qui estime qu'une telle interdiction généralisée des procédures de dé-anonymisation ne pourrait être mise en œuvre de manière efficace, notamment « en raison de la difficulté de détecter des ré-identifications secrètes motivées par l'appât du gain », voir OHM, p. 1758 s. tel que cité par MEIER, Big Data, p. 79.

818 Terme emprunté de l'ouvrage de l'économiste américaine ZUBOFF, pour une (longue définition) de ce champ émergent et florissant de l'économie, voir ZUBOFF, Surveillance Capitalism, Avant-propos ; si cette question n'est pas abordée dans le cadre de cette contribution, on consultera, pour des pistes intéressantes à ce sujet, GASSER qui cite quelques entreprises évoluant grâce à des traitements de données *Big Data* qui ont fait de la garantie de la sphère privée des personnes concernées un aspect central de leur *business model*. Ainsi, elles espèrent générer un avantage concurrentiel, voir GASSER, pp. 399 s. ; FLÜCKIGER avance quelques pistes de réflexion intéressantes quant à une éventuelle consécration d'un véritable droit de propriété sur les données personnelles ce qui aurait, entre autres, l'avantage de garantir un effet *erga omnes* du droit à l'autodétermination en matière informationnelle, voir FLÜCKIGER, pp. 858 ss. ; MEIER quant à lui reprend l'idée de monétarisation des données personnelles telle qu'avancée par FLÜCKIGER et mentionne, en outre, la possibilité de créer de nouvelles formes de coopération structurée entre des sociétés et des personnes concernées qui permettraient aux individus qui le souhaiteraient de confier leurs données à ces communautés d'utilisateurs selon un schéma de rétribution déterminé, voire de concevoir les données comme bien commun, voir MEIER, Big Data, pp. 86 ss. ; SCHMIDT enfin a dédié sa thèse soutenue en 2019 à l'Université de Bâle sur la manière dont le droit de la protection des données pourrait être développé vers un droit du commerce de données personnelles. Cette auteure considère que la consécration d'un véritable droit de propriété sur les données personnelles ne contribuerait pas à améliorer la protection de la personnalité des personnes concernées, bien au contraire. Pour ses conclusions nuancées, voir SCHMIDT, pp. 174 ss.

Ensuite, le pouvoir judiciaire appelé à trancher un litige est tenu d'interpréter les notions vagues à la lumière de l'art. 13 al. 2 Cst.

b. L'interprétation conforme des notions vagues

En vertu de l'art. 1er LPD, la LPD encadre uniquement les traitements de données personnelles dans la mesure où la LPD a vocation à protéger la personnalité et les droits fondamentaux des personnes concernées par un traitement et non les données elles-mêmes[819]. La notion de « donnée personnelle », qui n'a subi aucune modification dans le cadre de la révision totale, est donc une notion clé du droit de la protection des données.

Le profilage soulève de nouvelles questions quant à savoir quelles données constituent des données personnelles dont le traitement sera soumis à la LPD et lesquelles, au contraire, ne sauraient tomber sous la définition de « donnée personnelle » permettant ainsi au responsable du traitement, en l'occurrence l'employeur, de ne pas respecter les exigences de la LPD. Confronté aux nouveaux traitements de données et à leurs impacts sur les droits protégés des personnes concernées, le Tribunal fédéral a déjà été appelé, par le passé, à adapter la définition de « donnée personnelle » et a, de par son interprétation, élargi le champ d'application de la LPD[820]. Dès lors, il convient de réfléchir si une adaptation jurisprudentielle de cette notion dans le cadre d'un profilage pourrait contribuer à une meilleure protection des droits des candidats.

Les traitements de données anonymes ne pouvant porter atteinte à un quelconque droit de la personnalité ou à un quelconque droit fondamental, les lois pertinentes ne s'appliquent pas à ces traitements. Le principe selon lequel les traitements de données anonymes (qui restent anonymes)[821] ne devraient pas être encadrés par la LPD se justifie également dans la mesure où

819 La notion de « droit de la protection des données » peut prêter à confusion dans la mesure où elle peut laisser penser que cette branche du droit a vocation à protéger les données quand bien même cette branche juridique a pour but de garantir le respect de la personnalité des personnes dont les données sont traitées ; voir, pour les implications de cette notion souvent mal comprise, PRANTL, pp. 347 ss.

820 ATF 136 II 508, cons. 3.3 ss. Dans cette affaire connue sous le nom de « Logistep », le Tribunal fédéral a précisé que l'adresse IP (soit la suite de chiffres permettant d'identifier un utilisateur sur Internet) est une donnée personnelle protégée par la sphère privée. Dès lors, une entreprise privée comme p. ex. *Logistep* ne peut pas se substituer à la police pour les récolter.

821 Une analyse plus approfondie de l'efficacité des techniques d'anonymisation dépasserait le cadre de la présente contribution. On notera toutefois qu'elle est très sérieusement remise en cause, voir, avec des références supplémentaires, MEIER, Big Data, p. 69 ; à juste titre, HEUBERGER fait valoir que l'efficacité de ces techniques est tout particulièrement remise en cause dans le cadre du profilage dans la mesure où le but du profilage est précisément d'identifier une personne, directement ou indirectement, voir HEUBERGER, N 392.

il contribue à ne pas entraver la recherche et les évaluations statistiques des entités publiques et privées qui doivent déterminer si une mesure politique ou économique a été efficace sur la base de telles évaluations[822].

Or, comme nous l'avons vu plus haut[823], le profilage peut, dans certaines hypothèses, être effectué sur la base de données anonymes qui deviennent des données personnelles au cours du traitement (dé-anonymisation). Il est évident, qu'en théorie, le cadre légal s'applique dès que les données traitées permettent d'identifier le candidat. En pratique cependant, il n'est pas toujours aisé de déterminer avec précision à partir de quel moment le cadre légal doit être respecté[824]. Ainsi, afin d'améliorer la protection juridique des candidats et d'augmenter la sécurité juridique, il pourrait s'avérer judicieux d'élargir la notion de « donnée personnelle ». En d'autres termes, le Tribunal fédéral pourrait, dans le cadre d'une interprétation de la LPD à la lumière de l'art. 13 al. 2 Cst., retenir que dès qu'une donnée anonyme a le *potentiel* de devenir une donnée personnelle, le traitement effectué sur la base de cette donnée doit être qualifié de traitement de données personnelles. Une telle interprétation de la notion de « donnée personnelle » impliquerait alors que le cadre légal prévu par la LPD doit être respecté à partir du moment où le courtier en données acquiert des données anonymes dans le but de les évaluer et de rapporter l'évaluation faite à une personne individuelle[825]. Une extension de la notion de « donnée personnelle » et par là du champ d'application de la LPD[826] aurait pour conséquence d'encadrer la pratique des courtiers en données à partir du moment où les données anonymes risquent de devenir des données personnelles. Toutefois,

822 Pour un résumé du cadre spécifique en matière de recherche, voir PFPDT, Recherche, non daté ; pour un très bref résumé du cadre spécifique en matière de statistiques, voir PFPDT, Statistique, non daté.

823 Voir *supra* Chapitre 2. La définition compliquée du profilage.

824 MEIER, Big Data, p. 68 ; dans le même sens, voir ROUVROY, p. 21. Toutefois, ROUVROY avance une difficulté supplémentaire quant à une éventuelle implémentation de cette approche. En effet, elle soulève la question épineuse de savoir comment déterminer le responsable du traitement au sens de la législation pertinente en amont à un traitement de données anonymes qui aboutirait à un profilage.

825 Il convient de rappeler qu'un courtier en données peut également acquérir des données afin de les évaluer anonymement, p. ex. dans le seul but de déterminer des corrélations sans rapporter l'évaluation effectuée à des personnes individuelles, voir, à titre d'exemple, ROUVROY, p. 10.

826 Sans explicitement prendre position par rapport aux traitements de données anonymes, mais plaidant pour un élargissement du champ de protection de l'(a)LPD, voir WALTER, Perspectives, N 12. On notera que cette prise de position semble toujours être pertinente dans la mesure où la révision de la LPD n'a pas conduit à modifier le champ de protection (hormis l'exclusion de la protection des données des personnes morales).

comme MEIER et ROUVROY le soulignent à juste titre[827], l'extension du champ d'application de la LPD aurait pour conséquence d'accentuer le problème du consentement (et potentiellement des autres motifs justificatifs). Toutes les données matérielles ou anonymes devraient également faire partie de l'objet du contrat et/ou des conditions générales[828]. Les motifs justificatifs devraient alors porter sur celles-ci aussi[829]. De plus, une telle extension généralisée du champ d'application de la LPD impliquerait que l'« on fasse définitivement triompher les intérêts individuels (parfois très théoriques) sur les autres intérêts en jeu »[830]. Dans le cas d'un profilage effectué pendant la procédure d'embauche, cette réserve émise par MEIER ne saurait toutefois entièrement convaincre. Un élargissement du régime de protection aux traitements de données anonymes effectués par un employeur devrait être examiné[831], même si une telle approche sectorielle ajouterait une complexité à une matière déjà très complexe[832].

Hormis la notion de « donnée personnelle », qui est au cœur du débat relatif aux nouvelles technologies, la notion de « profilage à risque élevé » devra sans doute aussi être précisée par le pouvoir judiciaire.

Au vu des développements figurant dans la deuxième partie de cette contribution, il est important que le Tribunal fédéral définisse plus précisément la notion de « profilage à risque élevé » dans la mesure où la LPD et l'OPDo ne contiennent que peu d'indications quant à ses contours exacts. La notion de « risque élevé » devrait être interprétée généreusement, d'autant plus que le Conseil fédéral constatait en 2017 déjà que le profilage effectué sur le lieu de travail n'était que partiellement encadré. Ce faisant, il pourrait s'inspirer de

827 MEIER, Big Data, pp. 68 s. ; ROUVROY, p. 21.

828 MEIER, Big Data, p. 68.

829 Contrairement au droit européen et aux exigences du Conseil de l'Europe, la LPD permet d'effectuer des traitements de données sans motif justificatif, notamment à condition que les traitements soient conformes aux principes généraux. Toutefois, en raison de la nature vague de ces principes généraux, certains responsables de traitement ont la coutume de fonder tous leurs traitements sur un des motifs justificatifs prévus, notamment afin de s'assurer en cas de litige.

830 MEIER, Big Data, p. 68.

831 Sans toutefois prendre position spécifiquement par rapport au profilage et/ou au droit du travail, WALTER estime qu'« il est souhaitable de prévoir des règles particulières par rapport à certaines technologies ou types de traitements particulièrement invasifs », voir WALTER, Perspectives, N 11.

832 HEUBERGER fait valoir que les techniques d'anonymisation ne sont pas efficaces en matière de profilage. Dès lors, afin de protéger la personnalité des personnes concernées, il propose d'effectuer des profilages sur la base de données pseudonymisées, dont le traitement est soumis à la LPD. En d'autres termes, il semble défendre la position selon laquelle toute forme de profilage est soumise à la LPD. Toutefois, il ne précise pas comment concilier cette position avec les exigences liées au consentement ou aux autres motifs justificatifs, voir HEUBERGER, N 394.

la Recommandation profilage 2010 révisée par le Comité des Ministres en novembre 2021. Toutefois, même si le Tribunal fédéral adopte une interprétation généreuse de cette notion, les conséquences d'une telle interprétation seront très modestes en pratique. En effet, le Législateur n'a prévu qu'un régime (très légèrement) renforcé du profilage à risque élevé.

Au même titre que l'interprétation généreuse de la notion de « profilage à risque élevé », une interprétation généreuse des champs d'application des art. 328 CO et 328b CO s'impose. Une interprétation à la lumière de l'art. 13 al. 2 Cst. des champs d'application de ces deux dispositions est également de mise.

De surcroît, le pouvoir judiciaire pourrait être tenté de développer une règle par substitution, notamment dans les cas où ni une interprétation conforme ni le régime prévu ne parviennent à garantir les droits des candidats. En d'autres termes, on peut se demander si le Tribunal fédéral pourrait développer de nouvelles règles par substitution, voire « faire un pas supplémentaire »[833] et arriver à la conclusion que face aux nouveaux traitements de données automatisés qui impactent l'accès au marché du travail, l'art. 13 al. 2 Cst. produit un effet horizontal direct.

c. La consécration d'un effet horizontal direct

Il découle des quelques observations sommaires mentionnées en guise d'introduction, qu'une mesure de surveillance privée, comme p. ex. un profilage effectué pendant une procédure d'embauche, est potentiellement plus intrusive qu'une mesure de surveillance publique mise en place par les services de renseignement[834]. Toutefois, contrairement au profilage effectué par une entité privée, un profilage mis en place par un organe de l'État sera incontestablement encadré par différents droits fondamentaux, entre autres par le droit fondamental à l'autodétermination en matière informationnelle et diverses garanties procédurales.

Ainsi, il semble nécessaire de se demander si l'art. 13 al. 2 Cst. devrait avoir non seulement un effet horizontal *indirect*, mais aussi un effet horizontal *direct*. Quant à savoir si d'autres droits fondamentaux que celui consacré à l'art. 8 al. 3 3ème phrase se prêtent à une application directe entre privés, la doctrine est partagée[835]. La majorité de la doctrine ne considère toutefois pas que

833 MARTENET, art. 35 Cst., N 83.

834 Voir *supra* Chapitre 1. D'une surveillance publique à une surveillance privée.

835 DUBEY mentionne la liberté d'association positive et négative, la liberté syndicale positive et négative et le droit de grève, voir DUBEY, § 3, N 148 ; MARTENET quant à lui écrit qu'« une évolution vers une horizontalité directe ou quasi directe des art. 10 al. 3 Cst., 15 al. 4 Cst., 17 al. 3 Cst. et 28 al. 3 Cst. notamment ne paraît pas exclue, même si la jurisprudence est soit inexistante soit embryonnaire à cet égard, voire équivoque », voir MARTENET, art. 35 Cst., N 81, avec de multiples références supplémentaires.

l'art. 13 al. 2 Cst. devrait avoir un tel effet[836] même si un tel effet de toute ou partie de cette disposition constitutionnelle ne semble pas être exclu en théorie[837]. BELSER quant à elle fait valoir qu'une lecture littérale de l'art. 13 al. 2 Cst. aurait l'avantage d'éviter les conflits entre les différentes dispositions constitutionnelles éventuellement applicables en matière de protection de la personnalité[838]. De plus, elle est d'avis qu'une application de cette disposition constitutionnelle à *tous* les traitements de données (et non aux seuls traitements de données abusifs) crée de fausses attentes auprès des personnes concernées et a conduit les responsables de traitement à mettre en place des compilations de règles privées (*Privatisierung der Gesetzgebung*)[839]. De surcroît, une lecture littérale de cette disposition constitutionnelle permettrait la consécration d'une protection à échelle variable, notamment en fonction de la personne concernée (personne physique ou morale), de l'usage abusif (ou non) du traitement de données ou de l'atteinte (ou pas) au noyau dur du droit fondamental à la protection des données personnelles. Ainsi, selon cette auteure, il serait plus en ligne avec les développements technologiques actuels d'adopter une lecture littérale de cette disposition et dès lors de restreindre son champ d'application. Consciente des atteintes potentiellement néfastes que peuvent porter les nouveaux traitements de données au droit consacré à l'art. 13 al. 2 Cst., elle propose de conférer un effet horizontal direct à cette disposition dans les hypothèses de traitements de données abusifs. En d'autres termes, elle considère qu'une lecture littérale de la disposition serait plus apte à protéger les droits fondamentaux des personnes concernées qu'une application de l'art. 13 al. 2 Cst. à tous les traitements de données, mais dépourvue d'un effet horizontal direct[840].

836 MEIER, Protection des données, N 24 ; FLÜCKIGER, p. 852 ; *a contrario* DUBEY, § 3, N 146 ss. ; dans le contexte du droit du travail, RUDOLPH considère que deux droits fondamentaux seulement déploient un effet horizontal direct entre employeur et employé (art. 8 al. 3 3ème phrase Cst. et 110 al. 3 Cst.), l'art. 13 al. 2 Cst. ne fait pas partie de cette courte liste, voir RUDOLPH, Richterliche Rechtsfindung, N 226 ss.

837 MARTENET, art. 35 Cst., N 84.

838 L'auteure elle-même concède toutefois que ces conflits de droits n'ont pas une portée déterminante en pratique et fait référence, sur ce point, à BIAGGINI, art. 10 Cst., N 17. Dans une contribution publiée deux ans plus tard, elle précise qu'une application de cette disposition à *tous* les traitements de données ne permet pas d'insérer cette disposition comme *lex specialis* au sein de la protection de la personnalité au niveau constitutionnel dans la mesure où tout traitement de données tombe automatiquement dans le champ de protection de l'art. 13 al. 2 Cst., voir BELSER, Tragweite des Grundrechts auf Datenschutz, pp. 36 s.

839 BELSER, Tragweite des Grundrechts auf Datenschutz, p. 35.

840 BELSER, § 6, N 168 ss. ; pour un résumé de la position de GÄCHTER et EGLI qui défendent une position encore plus « radicale » dans la mesure où ils proposent de renoncer au droit à l'autodétermination en matière informationnelle et de consacrer certaines garanties minimales au niveau constitutionnel, comme les principes de transparence

Si une telle lecture semble intéressante, elle ne saurait toutefois entièrement convaincre et ceci pour plusieurs raisons. D'abord, une telle lecture implique que la personne concernée qui souhaiterait se prévaloir de son droit consacré à l'art. 13 al. 2 Cst. doit apporter la preuve d'un « abus », notion extrême aux contours flous[841]. Au-delà des contours flous de la notion d'« abus », il n'est pas évident de savoir dans quelle mesure un profilage porte atteinte au noyau dur du droit à l'autodétermination en matière informationnelle. Dans ce contexte, on peut se demander si « le fait d'opposer mécaniquement les choix et les actions d'autres personnes à un être humain revient à le déposséder de sa propre liberté de choix et d'action[842] » et, dans l'affirmative, considérer que « cela porte atteinte d'une gravité extrême à sa liberté individuelle et à son droit d'autodétermination, dont [on] peut se demander si elle ne touche pas au noyau intangible de ces droits. Tous les algorithmes ne sont cependant pas directement concernés, mais seulement ceux qui tendent à faire des prédictions sur la personnalité et le comportement futur d'un individu »[843]. Si l'analyse de MONTAVON relative au potentiel noyau dur de cette disposition constitutionnelle est intéressante, elle suscite de nouvelles questions épineuses quant à savoir quels profilages doivent être considérés comme aboutissant à de telles prédictions et devraient être interdits et lesquels, au contraire, ne portent pas atteinte à ce noyau dur. En sus des difficultés liées aux moyens de preuve telles que décrites dans la deuxième partie de cette contribution, la lecture proposée par BELSER aurait vraisemblablement pour conséquence que dans le futur, la protection serait limitée à des cas exceptionnels. À juste titre, FLÜCKIGER souligne que « l'individu perdrait en fin de compte la maîtrise juridique de ses données personnelles, après en avoir déjà perdu la maîtrise de fait. Tombant

et de finalité, le droit d'accès et une institutionnalisation des moyens de surveillance, voir FASNACHT, N 124 ss. On notera la similitude entre la proposition de ces deux auteurs suisses et l'art. 8 al. 2 Charte ; pour une brève analyse critique de la doctrine minoritaire allemande qui propose la consécration d'un tel effet horizontal direct du droit à l'autodétermination en matière informationnelle, voir MARSCH, pp. 250 s.

841 FLÜCKIGER, p. 848.

842 Dans le même sens, mais adoptant une approche économique à la thématique (ce qui correspond d'ailleurs à sa formation), voir ZUBOFF, Big Other, p. 82.

843 À la suite de ces développements, MONTAVON cite l'exemple d'un profilage effectué par la justice pénale nécessairement soumis aux dispositions de droit public. À mon sens, ces développements peuvent également ouvrir une piste de réflexion dans le cadre de l'emploi, voir MONTAVON, p. 664 ; le Comité des Ministres s'exprime également sur un ton critique (mais moins tranchant) par rapport au fait d'opposer à un individu des données personnelles qui appartiennent à d'autres individus, voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 53 ; à défaut d'une définition du noyau intangible de l'art. 13 al. 2 Cst. et sans évoquer les nouvelles formes de traitements, FASNACHT propose deux approches sur ce qui constituerait ce noyau intangible. Il ne semble toutefois pas aller aussi loin que MONTAVON, voir FASNACHT, N 153.

en quelque sorte dans le ‘domaine public’, les données personnelles seraient ainsi, par exemple, mises à la libre disposition des grandes entreprises »[844]. De plus, une telle lecture serait contraire aux engagements internationaux de la Suisse dans la mesure où le standard de protection fixé en droit international est plus élevé que la seule limitation à l’utilisation abusive[845] et pourrait conduire le Législateur à s’abstenir de légiférer[846].

On pourrait être tenté de proposer la consécration de l’effet horizontal direct de cette disposition dans les hypothèses relevant du droit du travail, p. ex. En d’autres termes, le Tribunal fédéral pourrait être amené à décider dans quels secteurs juridiques, il souhaite garantir une protection plus importante des droits des personnes concernées. *In fine*, dans cette hypothèse également, il reviendrait au juge de procéder à la distinction entre les cas problématiques (que BELSER qualifie d’« abusif » en vertu du texte constitutionnel) et ceux qui ne le sont pas et impliquerait que les personnes concernées doivent prouver que le litige relève de cette branche juridique et mérite dès lors d’être adressé sur la base de l’effet horizontal direct de l’art. 13 al. 2 Cst.

Comme nous l’avons vu plus haut, les procédures judiciaires en droit de la protection des données sont rares, voire très rares, notamment en raison de l’opacité qui entoure les nouveaux traitements de données et du contexte particulier de la procédure d’embauche qui tend à décourager les personnes concernées à saisir le tribunal compétent. Or, la reconnaissance d’un effet horizontal direct, outre les difficultés théoriques, suppose l’existence de procédures judiciaires. À défaut d’une révision des voies de recours et d’un important travail de sensibilisation, une consécration éventuelle de l’effet horizontal direct de l’art. 13 al. 2 Cst. risque dès lors d’être utopique.

D. Conclusion intermédiaire

L’art. 13 al. 2 Cst., qui consacre le droit fondamental à l’autodétermination en matière informationnelle a incontestablement une portée entre particuliers. En effet, en adoptant la LPD (et d’autres dispositions spéciales comme p. ex. l’art. 328b CO), le Législateur a œuvré à la réalisation de cette disposition

844 FLÜCKIGER, p. 848.

845 FLÜCKIGER, p. 848.

846 Si MARTENET émet plusieurs réserves quant à la reconnaissance d’un effet horizontal direct de l’interdiction constitutionnelle de discrimination sur le lieu de travail, cette réserve valant, à mon sens, *mutatis mutandis* pour l’art. 13 al. 2 Cst., voir MARTENET, La protection, pp. 448 ss. ; dans une veine similaire, invoquant notamment la séparation des pouvoirs et ce qu’elle appelle la « coopération entre pouvoirs », voir BESSON, Humaniser le droit privé, p. 26.

constitutionnelle entre particuliers. Cela étant, il découle des développements ci-dessus que dans le cadre précis d'un profilage effectué lors d'une procédure d'embauche soumise au droit privé, le Législateur n'a *pas* su consacrer une protection efficace des intérêts fondamentaux des candidats que cette disposition constitutionnelle a pourtant vocation à protéger. En d'autres termes, il convient de constater que le Législateur suisse ne semble pas avoir su respecter *toutes* ses obligations positives qui découlent de l'art. 13 al. 2 Cst. Lors d'une violation d'une telle obligation, plusieurs conséquences juridiques sont envisageables.

D'abord, la violation d'une obligation positive peut être suivie d'une révision du cadre légal. Dans ce contexte, on pensera à une éventuelle précision de l'art. 328b CO qui porterait sur les traitements de données automatisés licites et le principe de transparence qui pourrait englober une obligation explicite de rendre le profilage transparent lors d'une procédure d'embauche, p. ex. dans les offres d'emploi. La définition légale de la « donnée personnelle sensible » doit être repensée, en tenant compte de la finalité et des circonstances du traitement. Un droit d'accès renforcé doit être consacré également dans l'hypothèse d'un profilage qui ne serait *pas* suivi d'une décision individuelle automatisée[847]. De surcroît, le candidat concerné devrait bénéficier d'un renversement du fardeau de la preuve[848]. Enfin, la consécration de la possibilité pour le PFPDT d'engager une procédure au nom et pour le compte des candidats concernés est indispensable afin de mettre en place une protection efficace des droits découlant de l'art. 13 al. 2 Cst.[849]. Dans la même veine, l'indépendance du PFPDT tant sur le plan financier que personnel doit être améliorée.

Ensuite, le pouvoir judiciaire pourrait être tenté de développer une règle par substitution, notamment dans les cas où ni une interprétation conforme ni le régime prévu ne parviennent à garantir les droits des candidats. En d'autres termes, on peut se demander si le Tribunal fédéral pourrait développer de nouvelles règles par substitution et ainsi consacrer un effet horizontal direct (partiel) de l'art. 13 al. 2 Cst. Reconnaître un effet horizontal direct à l'art. 13 al. 2 Cst. dans les relations précontractuelles de travail pourrait constituer une piste à suivre, notamment en raison des lacunes légales identifiées, de l'intensification de la surveillance émanant de particuliers et du risque d'évaluations identiques dans toutes les procédures d'embauche (si tous les

847 Pour un renforcement du droit d'accès lors d'un profilage, qui ne serait pas suivi d'une décision individuelle automatisée, voir WALTER, Perspectives, N 19.

848 Pour un renversement *généralisé* du fardeau de la preuve (solution qui me semble toutefois trop peu refléter les besoins en pratique), voir WALTER, Perspectives, N 23.

849 WALTER va même plus loin dans la mesure où il propose la mise en place de procédures (classiques) gratuites ainsi que la consécration de mécanismes de résolution des conflits alternatifs, comme p. ex. la médiation, voir WALTER, Perspectives, N 23.

recruteurs au sein d'un même secteur économique utilisent les mêmes logiciels d'évaluation) et être considéré comme une confirmation de l'approche dualiste qui caractérise la LPD. Toutefois, au-delà des réserves quant à l'insécurité juridique qu'entraînerait la consécration d'un tel effet horizontal direct, une telle consécration impliquerait que le candidat doive prouver une atteinte à son droit fondamental. Comme nous l'avons vu plus haut, apporter une telle preuve peut s'avérer compliqué en pratique. De plus, on rappellera que les procédures judiciaires en la matière sont très rares, notamment en raison de l'opacité qui entoure le profilage et du contexte spécifique qui tend à décourager les personnes concernées de saisir le tribunal compétent. Or, la reconnaissance d'un tel effet horizontal direct suppose que plusieurs procédures judiciaires soient engagées. Ainsi, la protection escomptée risque d'être très (ou que) théorique. En outre, on notera qu'un effet horizontal direct pourrait potentiellement porter atteinte à certains (autres) droits fondamentaux de l'employeur. Ainsi, même si la tentation de reconnaître un effet horizontal direct à cette disposition constitutionnelle est compréhensible, il découle des développements ci-dessus que la numérisation du monde du travail appelle des réponses nuancées et la mise en place de solutions préventives et non réactives. En d'autres termes, il est à espérer que cette disposition déploie des effets *erga omnes*, mais sur d'autres fondements que sur celui de la théorie des effets horizontaux directs.

Enfin (et surtout), le pouvoir judiciaire est appelé à interpréter les diverses dispositions de droit privé applicables au cas d'espèce à la lumière de l'art. 13 al. 2 Cst. Dans ce contexte, on pensera avant tout à la précision de la notion de profilage à risque élevé, à l'extension possible du champ d'application temporel de l'art. 328 CO ainsi qu'à celle du champ d'application matériel de l'art. 328b CO. Par ailleurs, il est légitime de se demander si le droit à l'autodétermination en matière informationnelle ne devrait pas lui-même être repensé. En effet, une approche plus dynamique prenant en compte la finalité et le contexte des profilages envisagés pourrait contribuer à une meilleure protection des intérêts fondamentaux des candidats. Au vu des conséquences (potentiellement problématiques) de la numérisation sur les relations précontractuelles de travail, le Tribunal fédéral semble devoir reprendre la création de droits fondamentaux non-écrits en matière de liberté personnelle, notamment si la Suisse ne souhaite pas faire l'objet d'une éventuelle condamnation de la part de la Cour EDH. Afin de déterminer le risque d'une telle condamnation, il convient dès lors d'analyser la jurisprudence de Strasbourg.

Chapitre 12.
Le cadre prévu par le Conseil de l'Europe

Lorsque la Cour EDH est amenée à juger une affaire relevant du droit de la protection des données, elle se fonde sur deux conventions. Elle fait appel à l'art. 8 CEDH qui consacre le droit au respect de la vie privée et familiale (A). Le champ d'application exact de cette disposition dans le cadre d'un litige portant sur une question relative au droit de la protection des données se déterminera toutefois en vertu de la Convention 108+[850]. La Convention 108+ a pour but de fixer un niveau de protection des données unifié dans tous les États signataires et de protéger le droit à la vie privée des personnes physiques (B). Même si les dispositions de cette Convention relèvent depuis plusieurs années de l'ordre juridique interne des États membres du Conseil de l'Europe[851], la complexité des questions relatives à la protection efficace des données personnelles appelle des analyses et des solutions innovatrices et adaptées aux différents secteurs économiques[852]. Ainsi, le Comité des Ministres peut adopter des recommandations fondées sur la Convention 108 à l'intention des États signataires[853]. Parmi les nombreuses recommandations qu'il a adoptées, l'une d'entre elle porte sur le profilage[854] et une autre sur les traitements de données qui peuvent être effectués par un employeur[855]. Ces deux dispositifs non-contraignants seront analysés dans un troisième et dernier temps (C).

850 SCHWEIZER R., Rechtsprechung des EGMR, p. 465.

851 Tous les États membres du Conseil de l'Europe ont ratifié la Convention 108, voir Conseil de l'Europe, état des signatures et ratifications du traité 108 ; en octobre 2022, 19 États avaient ratifié la Convention 108+, dont 17 États membres du Conseil de l'Europe, voir Conseil de l'Europe, état des signatures et ratifications du traité 223.

852 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 15.

853 Plus précisément, le Comité conventionnel composé de représentants des États membres (art. 22 al. 2 Convention 108+) peut faire des recommandations (art. 23 let. a Convention 108+) qui seront ensuite soumises au Comité des Ministres (art. 24 al. 2 Convention 108+).

854 Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage du 3 novembre 2021 remplaçant la Recommandation CM/Rec(2010)13 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage du 23 novembre 2010.

855 Recommandation CM/Rec(2015)5 sur le traitement des données à caractère personnel dans le cadre de l'emploi du 1er avril 2015.

A. Le droit au respect de la vie privée et familiale (art. 8 CEDH)

L'art. 8 al. 1er CEDH qui consacre le droit au respect de la vie privée et familiale se lit comme suit : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Ce droit n'est toutefois pas absolu et peut être restreint aux conditions fixées à l'art. 8 al. 2 CEDH.

Adoptée en 1950, cette disposition ne mentionne ni un quelconque droit à la protection des données ni une possible application pendant une relation de travail, voire en amont d'une telle relation. À son origine, l'art. 8 CEDH était conçu en tant qu'obligation négative incombant aux autorités publiques et devait protéger les individus contre toute ingérence injustifiée de la part des autorités publiques[856]. Ainsi, de prime abord, cette disposition ne vient pas garantir le respect d'un quelconque droit à la protection des données pendant une relation de travail et encore moins pendant une procédure d'embauche. Consciente que le droit à la protection des données constituait un des défis majeurs que devaient relever les démocraties libérales pendant la deuxième moitié du 20e siècle[857], la Commission européenne des droits de l'homme (qui a été remplacée en 1998 par la Cour EDH permanente)[858] a rendu les premiers arrêts en la matière (au sens large) dès les années 1960[859].

Très peu de temps après l'entrée en vigueur de la Convention 108 en 1981, la Cour EDH a estimé que tout traitement de données personnelles tombe dans le champ d'application de l'art. 8 CEDH – que les données traitées relèvent directement de la vie privée, voire familiale ou pas[860]. En effet, dans l'affaire

856 On notera que les rédacteurs de la CEDH avaient hésité à consacrer une obligation positive directement dans la CEDH, mais ont finalement renoncé à une consécration explicite d'une telle obligation (contrairement notamment à ce qui a pu être prévu dans la DUDH). La Cour EDH a ensuite fait découler des obligations positives de la CEDH dans sa jurisprudence, voir FROWEIN, art. 8 CEDH, N 2.

857 FROWEIN, art. 8 CEDH, N 1.

858 On rappellera que la Commission européenne des droits de l'homme, qui a siégé à Strasbourg de juillet 1954 à octobre 1999, est un organe qui, avec la Cour EDH et le Comité des Ministres, contrôlait le respect par les États membres des obligations découlant de la CEDH. La Commission a disparu lorsque la Cour EDH est devenue permanente en 1998 à la suite de l'entrée en vigueur du Protocole n° 11 à la CEDH, portant restructuration du mécanisme de contrôle établi par la Convention.

859 SCHWEIZER fait remonter la jurisprudence de la Cour EDH en matière de protection des données à un arrêt rendu en 1962, qui portait sur la prise de photos non-autorisée (cette affaire est non sans rappeler celle qui avait conduit les juristes WARREN et BRANDEIS à analyser la nécessité de consacrer un droit à la sphère privée en 1890 de l'autre côté de l'Atlantique), voir SCHWEIZER R., Rechtsprechung des EGMR, p. 467.

860 EPINEY/SCHLEISS, § 3, N 12 ; pour une plus ample analyse des limites imposées par la Convention 108+, voir *infra* Chapitre 12. Le cadre prévu par le Conseil de l'Europe.

Leander c. Suède[861] rendue en 1987, le requérant avait travaillé au musée naval de Karlskrona, qui se situait à côté d'une zone militaire interdite. Ses données liées à ses activités syndicales dans le passé figuraient dans un registre secret et avaient été à l'origine de son exclusion de l'emploi en question[862]. Si la Cour conclut que la mémorisation dans un registre secret et la communication de données relatives à la vie privée d'un individu entrent dans le champ d'application de l'art. 8 CEDH[863], elle estime toutefois que dans cette affaire, cette disposition n'a pas été violée. Les garanties mises en place par les autorités suédoises ont été jugées suffisantes et le gouvernement suédois était en droit de considérer que les intérêts de la sécurité nationale prévalaient sur les intérêts individuels du requérant[864].

En sus des obligations négatives de l'État, telles que reconnues dans l'arrêt *Leander c. Suède*, les juges de Strasbourg ont rapidement reconnu des obligations positives[865] lorsqu'est en cause une relation entre un particulier et un organe de l'État.

En effet, dans l'arrêt *Gaskin c. Royaume-Uni*[866] rendu en 1989, la Cour EDH consacre un droit d'accès aux dossiers établis par les services sociaux. Dans le cas d'espèce, les dossiers portaient sur des actes de maltraitance commis par les parents du requérant pendant son enfance[867]. La Cour EDH en a profité pour rappeler son approche sur l'existence d'une obligation positive dans un cas d'espèce[868].

Dans l'affaire *Niemietz c. Allemagne*[869] rendue trois ans plus tard, la Cour EDH consacre expressément le droit au respect de la vie privée dans le cadre d'une relation de travail soumise au droit privé[870] et en fait découler une obligation positive incombant aux pays membres du Conseil de l'Europe[871].

861 Cour EDH, *Leander c. Suède*, 26 mars 1987, n° 9248/81.

862 Cour EDH, *Leander c. Suède*, 26 mars 1987, n° 9248/81, §§ 14 ss.

863 Cour EDH, *Leander c. Suède*, 26 mars 1987, n° 9248/81, § 48.

864 Cour EDH, *Leander c. Suède*, 26 mars 1987, n° 9248/81, § 67.

865 La théorie dite des 'obligations positives' a été développée par la Cour EDH et implique que « l'action de l'État consiste […] à mettre en place des mesures nécessaires, y compris législatives, pour garantir le respect concret et effectif des droits découlant de l'article 8 de la CEDH », voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 4 ; la théorie des obligations positives est particulièrement importante lors de l'interprétation de l'art. 8 CEDH, voir KOKOTT/SOBOTTA, p. 226.

866 Cour EDH, *Gaskin c. Royaume-Uni*, 7 juillet 1989, n° 10454/83.

867 Cour EDH, *Gaskin c. Royaume-Uni*, 7 juillet 1989, n° 10454/83, § 49.

868 Cour EDH, *Gaskin c. Royaume-Uni*, 7 juillet 1989, n° 10454/83, § 42.

869 Cour EDH, *Niemitz c. Allemagne*, 16 décembre 1992, n° 13710/88.

870 Cour EDH, *Niemitz c. Allemagne*, 16 décembre 1992, n° 13710/88, §§ 29 ss.

871 Cour EDH, *Niemitz c. Allemagne*, 16 décembre 1992, n° 13710/88, § 37.

Les arrêts qui ont suivi sont venus préciser la portée du droit au respect de la vie privée sur le lieu de travail. Ainsi, dans l'affaire *Barbulescu c. Roumanie*[872], un employeur privé avait licencié le requérant après avoir surveillé puis lu ses communications électroniques. La Grande chambre de la Cour EDH a conclu que l'art. 8 CEDH avait été violé dans la mesure où il en découle une obligation positive à l'encontre des États. En effet, les États ont l'obligation de protéger le droit au respect de la vie privée et de la correspondance des employés sur leur lieu de travail. Dans cet arrêt, la Cour EDH estime avant tout que l'employé doit être informé, au préalable, de toute mesure de surveillance et que toute mesure mise en place doit se faire à la lumière du principe de proportionnalité[873].

Quelques années plus tard, la Grande chambre de la Cour EDH a une nouvelle fois été appelée à déterminer les contours de l'art. 8 CEDH dans un cas de surveillance privée sur le lieu de travail. Dans cet arrêt rendu en 2019[874], un employeur avait surveillé ses employées grâce à une caméra secrète installée au-dessus de la caisse du supermarché. Sur la base des données ainsi obtenues, qui permettaient de prouver des vols à grande échelle, les employées surveillées avaient été licenciées. Si la Grande chambre confirme que les États doivent œuvrer au respect du droit à une vie privée sur le lieu de travail[875], elle conclut néanmoins que les autorités espagnoles avaient su, dans cette affaire, trouver un bon équilibre entre les différents intérêts en cause et que dès lors, l'art. 8 CEDH n'avait pas été violé[876]. Si la Cour EDH confirme l'existence d'obligations positives[877], elle est plus réservée quant à l'étendue de l'obligation d'information. En effet, la Grande chambre estime que la mise en place d'une mesure de surveillance secrète était justifiée en raison des soupçons légitimes d'irrégularités graves et des pertes constatées. En d'autres termes, le devoir d'informer les personnes concernées d'une mesure de surveillance privée ne semble pas être absolu[878].

S'il est vrai que la Cour EDH a rendu quelques arrêts en matière de surveillance depuis l'affaire *López Ribalda et al. c. Espagne* en 2019, elle n'a pas été amenée à trancher un nouveau litige portant sur une mesure de surveillance

872 Cour EDH [GC], *Barbulescu c. Roumanie*, 5 septembre 2017, n° 61496/08.

873 Cour EDH [GC], *Barbulescu c. Roumanie*, 5 septembre 2017, n° 61496/08, §§ 78 et 133 ss.

874 Cour EDH [GC], *López Ribalda et al. c. Espagne*, 17 octobre 2019, n° 1874/13 et 8567/13.

875 Cour EDH [GC], *López Ribalda et al. c. Espagne*, 17 octobre 2019, n° 1874/13 et 8567/13, § 114 ss.

876 Cour EDH [GC], *López Ribalda et al. c. Espagne*, 17 octobre 2019, n° 1874/13 et 8567/13, §§ 123 ss. On notera toutefois que la Chambre était arrivée à la conclusion inverse en constatant une violation de l'art. 8 CEDH et une non-violation de l'art. 6 al. 1er CEDH, voir Cour EDH, *López Ribalda et al. c. Espagne*, 9 janvier 2018, n° 1874/13 et 8567/13, §§ 62 ss.

877 Cour EDH [GC], *López Ribalda et al. c. Espagne*, 17 octobre 2019, n° 1874/13 et 8567/13, § 118.

878 Cour EDH [GC], *López Ribalda et al. c. Espagne*, 17 octobre 2019, n° 1874/13 et 8567/13, § 131.

mise en place par un employeur soumis au droit privé, encore moins par un recruteur privé. S'il ne fait aucun doute que certaines obligations positives découlent de l'art. 8 al. 1er CEDH, notamment quant aux traitements de données qui peuvent être effectués sur le lieu de travail, il n'est que peu clair si et dans quelle mesure la Cour EDH souhaite encadrer les nouveaux traitements de données effectués de plus en plus fréquemment par les employeurs à travers l'Europe[879].

À ce titre, il convient de rappeler que la Cour EDH a mentionné la notion de profilage (soit « profiling » en anglais) dans 25 arrêts de chambre ou de Grande chambre seulement. Il est intéressant de relever que dans la plupart de ces arrêts, la Cour EDH s'est en effet penchée sur une possible violation de l'art. 8 CEDH. Toutefois, dans aucune de ces 25 affaires, la Cour EDH ne vient définir la notion[880]. Pour l'heure, elle n'a donc pas encore été amenée à déterminer le cadre qu'elle souhaite (éventuellement) donner au profilage en Europe. La notion n'apparaît pas non plus dans une des fiches thématiques pertinentes dans le cadre de cette contribution[881].

Il en va de même de la notion d'« intelligence artificielle » (« artificial intelligence » en anglais) ou celle de « décision automatisée » (« automatic decision » en anglais). En effet, il est quelques peu inquiétant que ni la Grande chambre ni une quelconque chambre de la Cour EDH ne se soit penchée sur la notion d'intelligence artificielle dans un de ses arrêts. Le juge PAVLI se réfère à cette nouvelle forme de traitement de données dans son opinion partiellement dissidente rédigée en annexe à l'arrêt *Einarsson et al. c. Islande* rendu en 2019 sans pour autant la définir. Dans cette affaire, les requérants faisaient valoir une violation de l'art. 6 al. 1er CEDH dans la mesure où ils n'avaient pas eu accès à toutes les données les concernant dans le cadre d'une procédure pénale. La procédure étant complexe, les autorités de poursuite avaient fait recours à une

---

879 Pour une étude menée en pleine pandémie révélant, entre autres, que 70% des employeurs contactés avaient mis en place ou envisageaient de mettre en place des nouvelles mesures de surveillance *pendant* la relation de travail, voir vmware, The Virtual Floorplan, New Rules for a New Era of Work, octobre 2021, p. 12. On notera que sur les 20 pays examinés, 10 sont membres du Conseil de l'Europe ; dans une veine plus optimiste, BERSET BIRCHER et MEIER estiment que parmi les différentes problématiques sur le lieu travail que la Cour EDH a pu adresser, c'est notamment en matière de surveillance des employés que l'impact de sa jurisprudence est le plus important, voir BERSET BIRCHER/MEIER, pp. 612 s.

880 Pour une analyse détaillée de cette jurisprudence, voir *supra* Chapitre 2. La définition compliquée du profilage.

881 Cour EDH, Unité de presse, Fiche thématique – Protection des données personnelles, septembre 2022, Cour EDH, Unité de presse, Fiche thématique – Surveillance au travail, janvier 2022 et Cour EDH, Unité de presse, Fiche thématique – Nouvelles technologies, septembre 2022. Il convient de noter que ces fiches ne lient pas la Cour, mais reflètent néanmoins quels arrêts sont importants selon la Cour EDH elle-même.

forme d'intelligence artificielle afin d'être en mesure d'analyser toutes les preuves. Contrairement à la majorité de ses collègues, le juge PAVLI estime que la mise en place de tels traitements de données pouvait porter atteinte aux droits garantis par l'art. 6 al. 1er CEDH, notamment si les requérants n'étaient pas en mesure de comprendre la démarche des autorités de poursuite[882].

La notion anglaise «automatic decision» est mentionnée à deux reprises[883]; la notion française de « décision automatisée » ne figure dans aucun arrêt à ce jour. Dans les deux arrêts rédigés en anglais, la notion ne se réfère toutefois pas à une forme de traitement de données automatisé, mais plutôt à une décision judiciaire prise *in abstracto*, c'est-à-dire sans appréciation des circonstances du cas d'espèce. En d'autres termes, la Cour EDH n'a pas (encore) été saisie d'un litige qui serait directement applicable à la thématique analysée dans la présente contribution.

Même si la Cour EDH n'a pas encore été appelée à définir une, voire plusieurs nouvelles formes de traitements de données automatisés, il n'en demeure pas moins que sa jurisprudence relative à la protection des données est abondante. Il n'y a aucune raison que certains droits que les juges de Strasbourg ont fait découler de l'art. 8 al. 1er CEDH ne trouvent pas application dans le cadre d'un profilage effectué lors d'une procédure d'embauche soumise au droit privé. Ainsi, on rappellera qu'il est de jurisprudence constante que toute forme de traitement de données tombe dans le champ d'application de l'art. 8 al. 1er CEDH[884]. Un profilage, même non-défini juridiquement, doit donc, en principe, répondre aux exigences qui découlent de cette disposition.

D'abord, tout comme en droit suisse, l'art. 8 al. 1er CEDH implique l'existence d'un droit d'accès aux données personnelles qui doit pouvoir être exercé dans le cadre d'une procédure équitable[885]. Même si la portée de ce droit dans un cas précis concernant deux particuliers reste peu claire[886], il ne fait aucun doute qu'un employeur qui effectue un profilage devra être en mesure de garantir l'exercice de ce droit au candidat qui en ferait la demande. Comme nous l'avons vu dans la première partie de cette contribution, l'exercice de ce droit peut se révéler compliqué en Suisse lorsqu'il s'agit d'accéder au raisonnement qui sous-tend un profilage (l'exercice de ce droit sera encore plus compliqué

882 Cour EDH, *Sigurdur Einarsson et al. c. Islande*, 4 septembre 2019, n° 39757/15, Opinion partiellement dissidente du Juge PAVLI, §§ 15 et 21.

883 Cour EDH, *Suso Musa c. Malte*, 23 juillet 2013, n° 42337/12, § 73 ; Cour EDH, *Velecka et al. c. Lituanie*, 26 juin 2019, n° 56998/16, 58761/16, 60072/16 et 72001/16.

884 SCHWEIZER R., Rechtsprechung des EGMR, p. 466.

885 Cour EDH, *Segerstedt-Wiberg et al. c. Suède*, 6 juin 2006, n° 62332/00, § 116 ss.

886 Cour EDH [GC], *Barbulescu c. Roumanie*, 5 septembre 2017, n° 61496/08.

lorsque le profilage a lieu à l'étranger). S'il ressort de la jurisprudence de la Cour EDH que le droit d'accès comprend, en aval, le droit de réfuter l'exactitude des données personnelles traitées[887], il appartiendra à la Cour EDH de déterminer les contours de ce « pilier du droit de la protection des données »[888], notamment en raison de la large marge de manœuvre laissée au pouvoir législatif des États membres du Conseil de l'Europe[889].

Ensuite, une mesure de surveillance cachée semble être, en principe, illicite. Dans quelques cas bien définis, la Cour EDH semble admettre des exceptions à cette interdiction. Dans le cadre d'un profilage (caché) lors d'une procédure de recrutement, il est difficilement concevable que la Cour EDH admette une exception comme dans l'affaire *López Ribalda et al. c. Espagne*. En d'autres termes, il faut s'attendre à ce que la Cour EDH impose un devoir d'information préalable.

De surcroît, il découle de la jurisprudence de la Cour EDH qu'il est insuffisant de consacrer certains principes, comme p. ex. celui de la sécurité des données, dans la législation nationale. Encore faut-il que ces garanties puissent être mises en œuvre de manière efficace[890]. Il va sans dire que la mise en œuvre de la LPD – même après sa révision totale – reste compliquée et que les sanctions pénales nouvellement introduites risquent de rester lettre morte[891]. Ainsi, il n'est pas certain que la LPD réponde à cette exigence découlant de l'art. 8 al. 1er CEDH.

Reprenant les développements de PULVER mentionnés plus haut et qui se fondent, entre autres, sur la jurisprudence de la Cour EDH, un traitement de données qui porterait atteinte aux droits consacrés par l'art. 8 al. 1er CEDH peut être justifié si les autorités disposaient de mesures aptes à prévenir la violation du droit fondamental, que les intérêts des tiers également concernés par la

887 Art. 9 al. 1er let. e Convention 108+ ; pour de plus amples développements relatifs au droit d'accès, y compris une analyse de la jurisprudence suisse et de la CJUE, voir SCHWEIZER R., art. 13 al. 2 Cst., N 85 s.

888 BIAGGINI a repris cette expression utilisée par SCHWEIZER R., voir BIAGGINI, art. 13 al. 2 Cst., N 14 et SCHWEIZER R., art. 13 al. 2 Cst., N 85 respectivement.

889 PULVER, p. 417 ; SCHWEIZER R., Rechtsprechung des EGMR, p. 457 ; pour les 27 États membres de l'UE la marge de manœuvre a été considérablement réduite avec l'entrée en vigueur du RGPD. Il est donc possible que la Cour EDH – si elle est appelée à préciser les contours du droit d'accès – s'inspire du droit d'accès tel qu'il est prévu dans le RGPD.

890 L'art. 13 CEDH garantit que « toute personne dont les droits et libertés reconnus dans la [CEDH] ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles » ; à titre d'exemple, on consultera Cour EDH, *Segerstedt-Wiberg et al. c. Suède*, 6 juin 2006, n° 62332/00, § 116 ss.

891 Voir *supra* Chapitre 8. La Loi sur la protection des données et Chapitre 9. Autres dispositifs fédéraux potentiellement applicables.

mesure litigieuse, comme p. ex. l'employeur, ou un intérêt public prépondérant ont été pris en compte et que le principe de proportionnalité a été respecté[892].

À la lumière des développements proposés plus haut à propos de l'art. 13 al. 2 Cst., il convient de rappeler que le profilage effectué par un employeur privé constitue un traitement de données personnelles qui porte atteinte au droit au respect de la sphère privée au sens de l'art. 8 CEDH, que diverses mesures législatives sont concevables afin d'encadrer ce traitement de données (mais que le Législateur a rejetées) et que les intérêts économiques de l'employeur ne sauraient primer sur le droit au respect de la sphère privée (et potentiellement d'autres droits fondamentaux) des candidats. Enfin et faisant suite à ce qui a pu être mentionné à propos du principe de proportionnalité[893], le profilage ne semble pas être proportionné au sens légal du terme, notamment en raison de l'incertitude qui entoure ce traitement de données qui permettrait de choisir le meilleur candidat pour un poste donné (aptitude de la mesure envisagée) et s'il peut raisonnablement être mis en place à l'encontre du candidat (proportionnalité au sens strict). En somme, un profilage effectué dans le cadre d'une procédure de recrutement soumise au droit privé ne semble donc pas être justifiable.

Le contenu exact des droits qui découlent de l'art. 8 al. 1er CEDH, notamment dans le contexte d'un profilage lors d'un recrutement reste incertain et sera, à défaut de définitions légales claires, défini au cas par cas par les juges de Strasbourg.

Au vu des défis actuels, il ne fait aucun doute que la jurisprudence de la Cour EDH devra encore se développer aussi et surtout en raison des dispositions nationales lacunaires. La Cour EDH, dans ces hypothèses, est alors l'instance de dernier recours pour les personnes concernées (à condition bien évidemment que les tribunaux nationaux n'aient pas eux-mêmes déjà interprété les dispositions constitutionnelles de manière extensive et ainsi mis fin au litige avant qu'il n'arrive à Strasbourg). Plusieurs ONG ont d'ailleurs tenté de contester des mesures de surveillance mises en place par les autorités *nationales* en engageant des recours, d'abord au niveau national puis devant la Cour EDH[894]. À mon avis, ce n'est qu'une question de temps jusqu'à ce que l'une d'entre elles remettent en cause des mesures de surveillance mises en place par des *privés*

892 PULVER, pp. 416 s.

893 Pour une analyse détaillée de la proportionnalité ou non d'un profilage, voir *supra* Chapitre 8. La Loi sur la protection des données.

894 Cour EDH [déc.], *Privacy International et al. c. Royaume-Uni*, 4 septembre 2020, n° 46259/16 ; Cour EDH [GC], *Big Brother Watch et al. c. Royaume-Uni*, 25 mai 2021, n° 58170/13, 62322/14 et 24960/15 ; Cour EDH [GC], *Centrum För Rättvisa c. Suède*, 25 mai 2021, n° 35252/08.

en saisissant les instances nationales avant de s'adresser à la Cour EDH. Cette évolution vers une remise en cause de la surveillance privée (sur le lieu de travail) semble être accentuée par le fait qu'elle concerne tous les États membres du Conseil de l'Europe[895]. En d'autres termes, la jurisprudence mentionnée et les développements technologiques cités en guise d'introduction sont la preuve qu'il s'agit d'une thématique européenne, voire mondiale (contrairement, p. ex., aux affaires portant sur les conditions de détention ou sur les contours de la liberté d'expression qui concernent avant tout certaines régions européennes[896]). Il est à espérer que les juges de Strasbourg procéderont alors à une clarification de la jurisprudence sur la base, entre autres, de la Convention 108+ révisée du Comité des Ministres.

B. La Convention 108 révisée

Bien que la Cour EDH ait consacré le droit de tout individu à ne pas faire l'objet d'un quelconque traitement de données (sous réserve d'être justifié) sur le fondement de l'art. 8 al. 1er CEDH dès les années 1960, les limites de cette disposition en matière de protection des données sont vite apparues. En effet, en raison des motifs justificatifs forcément très abstraits et les conditions d'un traitement de données licite peu claires, la Cour EDH ne pouvait pas garantir, à travers sa jurisprudence, la sécurité juridique nécessaire à ce domaine en pleine effervescence[897]. Ainsi, à la fin des années 1970, avant même l'ouverture du réseau Internet au public, la communauté internationale avait pris conscience qu'il était indispensable d'adopter des règles spécifiques en la matière permettant de trouver un juste équilibre entre la libre circulation des données (composante de la liberté d'information, elle-même composante de la liberté d'expression telle que consacrée par l'art. 10 CEDH) et les exigences découlant de l'art. 8 al. 1er CEDH[898]. La Convention pour la protection des personnes à l'égard

895 La surveillance privée est plus simple à mettre en œuvre simultanément dans différents pays. Au contraire, les mesures mises en place par les services de renseignement dépendent de décisions politiques nationales et diffèrent ainsi d'un pays à un autre. Cela étant, tous les services semblent avoir de plus en plus de compétences ; pour une brève analyse de la jurisprudence de la Cour EDH relative aux mesures de surveillance mises en place par le gouvernement du Royaume-Uni dans le cadre de la lutte contre le terrorisme et une appréciation critique de la LRens révisée suisse, voir HERTIG RANDALL/MARQUIS, art. 13 al. 1er Cst., N 57 ss.

896 Pour un aperçu récent des différentes violations de la CEDH par pays et par an, voir Cour EDH, Violation par article et par État 2020.

897 Rapport explicatif Convention 108, ch. 4.

898 MEIER, Protection des données, N 63.

du traitement automatisé des données à caractère personnel[899] (ci-après « Convention 108 ») a été adoptée, par les États membres du Conseil de l'Europe, au début des années 1980. Cette Convention avait pour but d'étendre le droit au respect de la vie privée des citoyens européens en prenant en compte l'augmentation des flux, nationaux et internationaux, de données personnelles au travers de traitements automatisés[900]. Il s'agit du premier instrument international contraignant au monde dans le domaine de la protection des données[901]. L'UE elle-même souhaite y adhérer, le Rapporteur spécial de l'ONU conseille la ratification à tous les États membres de l'ONU[902]. La Suisse quant à elle l'a ratifiée le 2 octobre 1997.

Contrairement à la CEDH, la Convention 108 est un traité international qui lie les États, sans pour autant créer des droits justiciables pour les privés. Elle ne prévoit donc aucun mécanisme supranational qui permettrait aux personnes physiques de faire recours en cas de violation de cette Convention. En d'autres termes, la Convention 108 n'a pas vocation à créer des droits justiciables, mais plutôt à harmoniser le niveau de protection entre les États signataires. Ainsi, la Convention 108 ne rend les art. 8 et 10 CEDH non pas obsolètes, mais vient, bien au contraire, complémenter la protection offerte par la CEDH[903]. En effet, en matière de protection des données, la Cour EDH détermine le champ d'application de l'art. 8 al. 1er CEDH en s'inspirant de celui de la Convention 108, respectivement de celui de la Convention 108 révisée.[904]

Au regard des développements susmentionnés[905], on retiendra que la Convention 108 révisée oblige les États à adopter une législation nationale encadrant, entre autres, les traitements de données personnelles automatisés effectués par des responsables soumis au droit privé[906], comme p. ex. les employeurs. En vertu de ce traité international, le cadre légal national doit prévoir, entre autres :

---

899 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, RS 0.235.1.

900 Convention 108, Préambule.

901 EPINEY/SCHLEISS, § 3, N 23.

902 Rapporteur spécial sur le droit à la vie privée, Rapport annuel A/73/438 à l'Assemblée générale des Nations Unies, recommandation 117.e.

903 EPINEY/SCHLEISS, § 3, N 26.

904 SCHWEIZER R., Rechtsprechung des EGMR, p. 465. On notera que contrairement à la CEDH, la Convention 108 s'applique expressément tant aux personnes privées qu'aux institutions publiques (art. 3 al. 1er Convention 108+).

905 Afin de faire face aux nouveaux développements technologiques, le Comité des Ministres a, en mai 2018, adopté un Protocole d'amendement à la Convention 108 (« Convention 108+ »), voir, pour plus de details, *supra*, Chapitre 2. La définition compliquée du profilage.

906 Art. 3 al. 1er Convention 108+.

— la consécration de divers principes généraux et des motifs justificatifs (art. 5, 7 et 8) ;
— un droit d'accès, qui porte, entre autres, sur le raisonnement qui sous-tend le traitement de données (art. 9 al. 1er let. c) ;
— le droit pour toute personne concernée de s'opposer, à tout moment, pour des raisons tenant à sa situation, à un traitement de données (art. 9 al. 1er let. d) ;
— un recours effectif (art. 12) ;
— la mise en place d'une autorité de surveillance indépendante (art. 15 ss.).

En revanche, la Convention 108+ n'oblige les États signataires ni à définir le profilage ni à encadrer ce traitement de données de manière spécifique en droit national[907]. En d'autres termes, la Convention 108+ n'impose pas la mise en place, en droit national, d'un encadrement juridique allant au-delà des principes généraux tels que prévus aux art. 5, 7 et 8 Convention 108+ et des droits des personnes concernées consacrés à l'art. 9 Convention 108+. Cette constatation est d'autant plus regrettable que huit ans avant l'adoption du Protocole d'amendement, le Comité des Ministres avait déjà constaté que diverses formes de profilage, « largement répandues mais peu connues du grand public, étaient potentiellement constitutives d'une atteinte au respect de la vie privée des personnes concernées »[908] et avait décidé d'adopter la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Cette Recommandation avait pour but de proposer des mesures juridiques permettant de mieux protéger les droits des personnes contre les risques posés par cette nouvelle forme de traitement de données. Constatant que la situation a considérablement évolué depuis l'adoption de cette Recommandation en 2010, le Comité des Ministres l'a révisée et a adressé une version retravaillée aux États membres en novembre 2021. Avant l'adoption du Protocole d'amendement, le Comité des Ministres avait également adressé une (autre) Recommandation aux États membres proposant un encadrement possible des nouveaux traitements de données effectués sur le lieu de travail.

907 L'art. 6 Convention 108+ fixe que des garanties appropriées venant compléter celles de la Convention 108+ doivent être prévues par une loi nationale. En d'autres termes, le traitement de données sensibles implique la mise en place d'un régime plus protecteur, mais non le profilage ; pour une analyse quant aux aspects problématiques de la notion de donnée personnelle sensible, notamment dans le cadre d'un profilage, voir *supra* Chapitre 11. Le cadre constitutionnel suisse.

908 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 20.

C. Les Recommandations du Comité des Ministres : CM/Rec(2021)8 sur le profilage et CM/Rec(2015)5 sur l'emploi

Même si les dispositions de la Convention 108 relèvent depuis plusieurs années de l'ordre juridique interne des États membres du Conseil de l'Europe[909], la complexité des questions relatives à la protection efficace des données personnelles appelle des analyses et des solutions innovatrices et adaptées aux différents secteurs économiques[910]. Ainsi, le Comité des Ministres – institution chargée d'assurer la représentation nationale des États membres au sein du Conseil de l'Europe – peut adopter des recommandations fondées sur la Convention 108 à l'intention des États membres[911]. Il a adopté plusieurs recommandations fondées sur la Convention 108 qui ont toutes pour but de garantir que la collecte et le traitement de données dans un secteur particulier (emploi, banque, assurance, santé, police etc.) ou effectués à l'aide d'une technologie particulière (carte à puce, vidéosurveillance, marketing direct etc.) ou encore relatifs à une catégorie particulière de données (sensibles, biométriques etc.) soient toujours conformes aux principes généraux énoncés dans la Convention 108[912]. Dans ce contexte, le Comité des Ministres a, entre autres, adopté la Recommandation profilage 2010[913] le 23 novembre 2010 déjà[914].

Conscient de l'utilisation croissante des nouvelles formes de traitements de données dans les relations entre employeurs et employés, le Comité des Ministres a estimé, quelques années plus tard, que ces nouveaux traitements de données devaient être gouvernés par des principes destinés à réduire les

909 Tous les États membres du Conseil de l'Europe ont ratifié la Convention 108, voir Conseil de l'Europe, état des signatures et ratifications du traité 108 ; en octobre 2022, 19 États avaient ratifié la Convention 108+, dont 17 États membres du Conseil de l'Europe, voir Conseil de l'Europe, état des signatures et ratifications du traité 223.

910 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 15.

911 Plus précisément, le Comité conventionnel composé de représentants des États membres (art. 22 al. 2 Convention 108+) peut faire des recommandations (art. 23 let. a Convention 108+), qui seront ensuite soumises au Comité des Ministres (art. 24 al. 2 Convention 108+). Les conclusions du Comité des Ministres peuvent ensuite, s'il y a lieu, revêtir la forme de recommandations aux Gouvernements. Le Comité peut inviter ceux-ci à lui faire connaître la suite donnée par eux aux recommandations (art. 15 let. b Statut du Conseil de l'Europe).

912 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 16. Une liste actuelle de toutes les recommandations adoptées par le Comité des Ministres peut être consultée sur le site du Conseil de l'Europe, voir Conseil de l'Europe, Protection des données, Instruments juridiques, Recommandations du Comité des Ministres.

913 On notera que cette abréviation ainsi que les deux abréviations suivantes couvrent tant la Recommandation à proprement parler que son Annexe.

914 Voir, pour plus de détails, *supra* Chapitre 2. La définition compliquée du profilage.

risques qu'ils pourraient éventuellement présenter pour les droits et libertés fondamentales des employés[915]. Ainsi, le 1er avril 2015, il a adopté la Recommandation CM/Rec(2015)5 sur le traitement des données à caractère personnel dans le cadre de l'emploi (ci-après « Recommandation emploi »).

En guise de rappel, on notera que la définition proposée par le Comité des Ministres a été retravaillée en profondeur dans le cadre des travaux de révision qui ont conduit à l'adoption de la Recommandation profilage 2021[916]. Désormais, les trois définitions du profilage potentiellement applicables en Suisse[917] sont (matériellement) identiques. Le « profilage à risque élevé » n'est désormais plus une spécificité suisse[918]. En effet, la Recommandation profilage 2021 introduit cette notion en son art. 1.1. let. j. Contrairement au droit suisse, cette disposition prévoit toutefois une liste non-exhaustive d'hypothèses dans lesquelles un tel profilage doit être admis.

En son article 5.5, la Recommandation profilage 2021 fixe que si une personne est soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur la seule base d'un profilage, elle devrait, en principe, pouvoir s'opposer à cette décision. Ce droit d'opposition n'est toutefois pas absolu. En effet, ce principe connaît des exceptions, notamment lorsque la décision ainsi prise est opérée dans le cadre de mesures précontractuelles. L'Exposé des motifs relatif à la Recommandation profilage 2010[919] précise à ce sujet que « le recours au profilage pour des décisions d'embauche est possible moyennant des garanties appropriées permettant à la personne concernée de faire valoir son point de vue, en particulier au cours d'un entretien où elle aura l'opportunité de démontrer l'inexactitude de données entrant dans son profil, l'inadéquation du profil à sa situation particulière, voire d'autres arguments »[920]. Or, on notera que les « garanties appropriées » telles que proposées par le Comité permettant de déroger au droit d'opposition du candidat sont dépourvues de sens pratique dans la mesure où le profilage est précisément mis en place pour économiser des ressources, c'est-à-dire pour éviter de devoir procéder à de nombreux entretiens d'embauche. En pratique, si la candidature d'une personne n'est pas retenue en raison d'un profilage effectué, la personne

915 Recommandation emploi, Préambule.

916 Voir, pour plus de détails, *supra* Chapitre 2. La définition compliquée du profilage.

917 Voir *supra* Méthodologie.

918 Pour une analyse plus approfondie des différences entre les diverses définitions du profilage potentiellement applicables en droit suisse, voir *supra* Chapitre 2. La définition compliquée du profilage.

919 Sur ce point, l'Exposé des motifs relatif à la Recommandation profilage 2010 semble toujours être pertinent.

920 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 149.

concernée ne sera pas même invitée à un entretien. Ce droit de faire opposition tel que fixé dans la Recommandation profilage 2010 puis légèrement précisé dans sa version révisée[921], risque dès lors de rester lettre morte. On rappellera également que le droit de faire valoir son point de vue n'a qu'un sens si le raisonnement qui sous-tend le profilage litigieux est compréhensible pour la personne concernée. Or, au vu de la complexité des raisonnements qui sous-tendent les profilages, il n'est pas certain qu'une reconnaissance même généralisée du droit de faire valoir son point de vue améliore considérablement les droits des candidats concernés.

Quant au devoir d'informer, la Recommandation profilage 2021 précise, à juste titre, que « lorsque les données à caractère personnel précédemment collectées sans intention d'appliquer des méthodes de profilage sont ensuite traitées de manière licite dans le cadre du profilage, le responsable du traitement devrait être tenu de donner les informations visées [par la Recommandation] »[922]. L'application de cette recommandation aux hypothèses pertinentes dans le cadre de cette contribution aurait pour conséquence que l'employeur qui acquiert une évaluation faite sur la base de données collectées dans un autre contexte que celui de la procédure d'embauche, devrait fournir toutes les informations mentionnées par la Recommandation profilage 2021 au candidat concerné. Il va sans dire qu'il n'est que peu certain qu'un employeur dispose de ces informations et les transmette en temps utile au candidat. Comme nous l'avons vu plus haut[923], aucune disposition légale allant au-delà des principes généraux ne vient implémenter cette recommandation en droit suisse.

Malgré les réserves émises à juste titre par MEIER et ROUVROY[924] quant à une éventuelle extension de la notion de « donnée personnelle », il est intéressant de noter que dans son Exposé des motifs, le Comité des Ministres proposait, en 2010 déjà, d'étendre, ne serait-ce qu'accessoirement, la notion de « donnée personnelle » et par-là le champ d'application de la Recommandation profilage 2010[925]. Dans sa version révisée, cette extension du champ d'application

921 À cette fin, on comparera les art. 5.3 Recommandation profilage 2010 et 5.5 Recommandation profilage 2021.

922 Art. 4.4 Recommandation profilage 2021 ; on notera que l'Exposé des motifs relatif à la Recommandation profilage 2010 prévoyait déjà une obligation allant dans ce sens, elle ne faisait toutefois pas partie de la Recommandation elle-même, voir Exposé des motifs relatif à la Recommandation 2010, pt. 135.

923 Voir *supra* Chapitre 10. Conclusion de la deuxième partie.

924 Pour une analyse plus approfondie de ces réserves, voir *supra* Chapitre 11. Le cadre constitutionnel suisse.

925 En effet, le Comité des Ministres précisait à propos de la définition de donnée personnelle dans le cadre du profilage que « de nombreuses caractéristiques individuelles décrivent le comportement des individus. À partir du moment où ces caractéristiques sont nombreuses et précises, il devient possible d'identifier chaque individu en particulier sur la

a même été consacrée de manière expresse. En effet, l'art. 2.3 fixe qu'« avec des traitements automatisés [...] il est difficile de savoir *a priori* quelles données permettront des corrélations ou des prédictions relatives à une personne concernée. Dans de tels cas, pour que les données à caractère personnel soient traitées de façon loyale, les organisations devraient garantir la pertinence et la qualité de toutes les données, y compris les données non personnelles, qui pourraient permettre les corrélations ou prédictions relatives à une personne concernée ». L'application de ces cautionnements à un profilage effectué dans le cadre d'une procédure d'embauche aurait pour conséquence que l'employeur en tant que responsable du traitement ne saurait se fier à un sous-traitant qui affirme que le profil créé par ses soins est forcément licite dans la mesure où il a été généré sur la base de données anonymes.

Tel qu'évoqué dans la deuxième partie de cette contribution, il n'est pas toujours clair de savoir si un profilage est conforme au principe de proportionnalité, qui impose, entre autres, que le traitement de données envisagé soit nécessaire[926]. À cet égard, l'Exposé des motifs relatif à la Recommandation 2010 précisait déjà qu'un profilage puise sa légitimité, entre autres, dans l'application de mesures précontractuelles. Le Comité des Ministres émettait toutefois une réserve importante en précisant que le profilage « doit apparaître nécessaire pour [...] l'application de mesures précontractuelles »[927]. En d'autres termes, un profilage ne peut être effectué dans tous les contextes précontractuels : il incombe au responsable du traitement de démontrer la nécessité d'un tel traitement de données. Dans le cas des procédures d'embauche, il

base du comportement qui lui est propre et unique. Dans le cadre du profilage, un individu n'est véritablement anonyme que si la valeur des données recueillies à son sujet n'est pas unique – en d'autres termes, si deux individus différents dans un contexte donné possèdent les mêmes caractéristiques » et d'ajouter, à propos de la définition du profilage, que « la première étape [d'un profilage] consiste à collecter sur une grande échelle des données relatives à des comportements individuels. Il peut s'agir d'un panier d'achat, d'un relevé de télécommunications, d'une liste de déplacements dans les transports publics, etc. Les données relatives à ces comportements individuels peuvent être anonymisées ou codées ». Dans une veine plus générale, le Comité des Ministres a tenu de rappeler qu'« au-delà de la stricte application de la Convention 108, il implique d'être attentif de manière plus large à la façon dont les techniques de profilage peuvent porter atteinte à la vie privée, entendue comme la capacité d'autodétermination des individus », voir Exposé des motifs relatif à la Recommandation profilage 2010, pt. 84, 96 et 105.

926 Voir *supra* Chapitre 8. La loi sur la protection des données.

927 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 119 ; la Recommandation profilage 2021 fixe désormais de manière explicite que le profilage « ne peut être effectué que [...] s'il est nécessaire aux fins de l'intérêt légitime du responsable du traitement ou du/des tiers auxquels le profil ou les données sont communiquées, à condition que ne prévalent pas les libertés et droits fondamentaux de la personne concernée [...]. La nécessité devrait être explicitement motivée par le responsable du traitement », voir l'art. 3.4 Recommandation profilage 2021.

découle des développements de la deuxième partie de cette contribution qu'il n'est pas certain que la nécessité du profilage puisse être démontrée de manière généralisée.

On relèvera en outre que la Recommandation profilage 2021 propose d'interdire la collecte et le traitement de données sensibles dans le cadre du profilage, sauf si ces données sont nécessaires pour les finalités légitimes et spécifiques du traitement et pour autant que le droit interne prévoie des mesures appropriées[928]. L'Exposé des motifs relatif à la Recommandation profilage 2010 précisait déjà que les garanties appropriées et légitimes peuvent consister, « p. ex., dans le consentement de la personne concernée ou dans l'encadrement par une loi du processus de profilage envisagé, afin de maintenir la confidentialité des données traitées ou résultant de l'opération de profilage, et de veiller à ce que l'utilisation des profils soit strictement réservée aux seuls traitements qui sont légitimes. Par ailleurs, le principe prévoit expressément la condition de consentement explicite au profilage lorsque celui-ci porte sur des données sensibles et requiert ainsi un consentement »[929]. Force est de constater que le régime légal suisse ne répond qu'en partie à ces exigences. Les diverses lois fédérales applicables pendant une procédure d'embauche ne contribuent pas à maintenir la confidentialité des données sensibles et n'empêchent que de manière très hypothétique l'utilisation abusive du profilage par un employeur un peu trop curieux. De même, on rappellera que le consentement explicite ne semble pas pouvoir être donné dans le cadre d'une procédure d'embauche, notamment en raison du lien de subordination naissant[930] et de la nature souvent invisible du profilage[931].

De surcroît, le Comité des Ministres propose des mesures strictes, notamment « d'interdire en principe le profilage de personnes ne pouvant librement exprimer leur consentement, en particulier, par exemple, les personnes atteintes d'incapacité ainsi que les enfants […]. Il est considéré qu'une telle interdiction de principe est nécessaire au vu des risques de manipulation et de discrimination négative que représente le profilage par rapport à ces catégories de personnes »[932]. On notera que « quand le profilage est fondé sur le consentement, il incombe au responsable du traitement de prouver que la personne concernée

928 Art. 3.11 Recommandation profilage 2010 ; ce principe est nouvellement consacré à l'art. 3.13 Recommandation profilage 2021.

929 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 130.

930 Pour une analyse plus approfondie de la nature du lien précontractuel qui lie l'employeur et le candidat en droit suisse, voir *supra* Chapitre 7. Le Code des obligations.

931 À titre d'exemple, voir Recommandation profilage 2010, cons. 3.

932 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 120 ; cette proposition a été légèrement reformulée et a été consacrée à l'art. 3.5 de la Recommandation profilage 2021.

a accepté explicitement le profilage au-delà de ce qui était nécessaire à l'exécution de la prestation et ce après avoir été informée conformément [aux conditions fixées par la Recommandation profilage 2021] »[933]. L'implémentation de cette recommandation en droit national aurait pour conséquence d'interdire le profilage de la plupart des apprentis, qui sont mineurs au moment de postuler pour un apprentissage.

On notera que l'art. 3.4 Recommandation profilage 2021 porte sur les conditions générales de licéité d'un profilage. En d'autres termes, ce principe fixe les motifs justificatifs potentiellement pertinents en cas de profilage. À ce titre, on relèvera que contrairement au droit suisse (même révisé), le profilage doit puiser sa légitimité dans un des motifs justificatifs mentionnés par cette disposition :

— le profilage est expressément prévu par une loi nationale[934] ;
— le consentement libre, spécifique, éclairé et non équivoque de la personne concernée (dans le cadre d'un profilage à risque élevé, le consentement doit être exprès[935]) ;
— le profilage est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'application de mesures précontractuelles prises à la demande de celle-ci ;
— un intérêt privé prépondérant du responsable du traitement ou d'un tiers auquel les données sont communiquées. Dans cette hypothèse, les rédacteurs de la Recommandation précisent que l'utilisation du profilage sera soumise à un double critère de légitimité dans la mesure où le responsable du traitement devra, d'abord, se demander si la finalité du profilage envisagé est légitime et si oui, s'il est légitime, pour atteindre cette finalité, de recourir au profilage[936] ;
— un intérêt public prépondérant (non-applicable dans le contexte d'une procédure d'embauche soumise au droit privé) ;
— la sauvegarde de l'intérêt vital de la personne concernée (non-applicable dans le contexte d'une procédure d'embauche soumise au droit privé).

933 Art. 3.6 Recommandation profilage 2021 ; dans le même sens déjà en 2010, voir l'art. 3.6 Recommandation profilage 2010.

934 On notera que ce motif justificatif a été introduit dans le cadre des travaux de révision ce qui laisse penser que les autorités publiques ont plus fréquemment recours au profilage qu'en 2010 et souhaitaient que ce motif justificatif figure dans la Recommandation profilage 2021.

935 On notera que cette précision a été introduite dans le cadre des travaux de révision dans la mesure où la notion de « profilage à risque élevé » est nouvelle. Ainsi, sur ce point, le régime suisse rejoint celui proposé par le Comité des Ministres.

936 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 119. Les développements qui y figurent portent sur les profilages effectués dans le cadre du marketing direct. Il n'existe aucune raison que ces développements ne sauraient être appliqués *mutatis mutandis* à un profilage effectué dans le cadre d'une procédure d'embauche.

Quant au principe d'exactitude particulièrement important dans le cadre d'un profilage, la Recommandation profilage 2021 précise que « le responsable du traitement et, le cas échéant, les sous-traitants devraient prendre des mesures appropriées pour corriger les facteurs d'inexactitude des données et limiter les risques d'erreurs et de biais inhérents au profilage »[937]. L'Exposé des motifs de 2010 précisait que cette obligation ne vaut non seulement pour les données personnelles mais aussi pour les données anonymes éventuellement traitées dans le cadre d'un profilage[938]. Désormais, cette obligation est expressément consacrée à l'art. 2.3 Recommandation profilage 2021. Même si l'extension de cette obligation aux données anonymes traitées semble pertinente en théorie, la portée pratique de cette recommandation devrait être modeste. Si elle n'est pas accompagnée d'un important effort de sensibilisation, la plupart des responsables de traitement habitués au « régime classique de la protection des données » n'accorderont pas une grande importance aux traitements de données anonymes et seront donc enclins à ignorer cette règle.

Dans une veine plus générale, il est fort intéressant de noter que contrairement à la jurisprudence de la Cour EDH, la Convention 108+ et la Recommandation profilage 2021 semblent consacrer une certaine idée de contrôle sur les données personnelles. Le Comité des Ministres estime qu'une certaine forme de contrôle est indispensable à l'exercice du droit à la vie privée et à la protection des données à caractère personnel qui supposent « l'existence de sphères de vie différentes et indépendantes où chaque individu peut contrôler l'usage des informations qui le concernent »[939]. Dans ses précisions relatives aux principes généraux, qui n'ont toutefois pas pour but de créer de nouvelles obligations légales[940], le Comité des Ministres rappelle que le profilage peut « porter atteinte à la vie privée, entendue comme la capacité d'autodétermination des individus »[941]. Ainsi, le Comité des Ministres semble faire référence au droit

937 Art. 3.10 Recommandation profilage 2021 ; une obligation similaire était déjà consacrée à l'art. 3.9 Recommandation profilage 2010. La distinction la plus importante réside dans le fait que la Recommandation profilage 2021 s'adresse non seulement aux responsables du traitement, mais aussi expressément aux sous-traitants potentiels.

938 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 126.

939 Recommandation profilage 2021, cons. 7 ; dans une veine très similaire, reflétant de manière plus précise les buts du droit à l'autodétermination en matière informationnelle, voir Recommandation profilage 2010, cons. 4. En effet, la version antérieure précisait que l'existence de sphères de vie différentes permettait à l'individu de contrôler l'usage qu'il ou elle souhaitait faire de *son identité* ; le Préambule de la Convention 108+ rappelle que l'autonomie personnelle est « fondée sur le droit de la personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait ».

940 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 103.

941 Exposé des motifs relatif à la Recommandation profilage 2010, pt. 105.

fondamental à l'autodétermination en matière informationnelle connu en droit constitutionnel suisse (et allemand). Reste à savoir si la Cour EDH consacrera explicitement ce droit dans sa future jurisprudence, p. ex. sur le fondement de la Recommandation profilage 2021, voire sur le Préambule de la Convention 108+[942].

S'il est vrai que la Recommandation emploi est considérablement plus longue que la Recommandation profilage 2021, il n'en reste pas moins qu'elle ne contient que peu de précisions quant aux traitements de données qui peuvent être effectués dans le cadre d'une procédure d'embauche. La Recommandation emploi vient préciser le principe de transparence en prévoyant que lorsque l'employeur traite des données collectées auprès de tiers, p. ex. dans le but d'obtenir des références professionnelles, le candidat doit être dûment informé au préalable[943]. À condition que le *data broker* soit qualifié de tiers, un profilage effectué à l'insu du candidat serait dès lors contraire au principe de transparence.

De plus, la Recommandation emploi consacre une interdiction de principe de tout traitement de données de santé, voire de données génétiques. Or, le profilage peut révéler des données de santé sur la base de données non-sensibles, voire des données qui n'ont aucun lien apparent avec le domaine médical[944]. Dès lors, un profilage qui aboutirait à une information relative à l'état de santé du candidat serait interdit (à moins de répondre à l'une des exceptions prévues[945]).

Enfin, on notera que le Comité des Ministres considère que les tests psychologiques destinés à évaluer le caractère ou la personnalité d'un candidat ne devraient qu'être effectués par des professionnels spécialisés, soumis au secret médical. Le profilage a précisément pour but d'évaluer la personnalité

942 En 2013, FLÜCKIGER précisait à ce sujet que la Cour EDH « n'a à ce jour pas explicitement reconnu un droit indépendant à l'autodétermination informationnelle. Elle n'en serait toutefois plus très éloignée […]. L'autodétermination est en effet un principe qui sous-tend implicitement l'ensemble de la jurisprudence relative à la protection des données. Le Tribunal fédéral en fait la même lecture puisqu'il se réfère également à l'art. 8 CEDH pour fonder le droit à l'autodétermination », voir, avec des références supplémentaires, FLÜCKIGER, p. 845.

943 Art. 5.1 Recommandation emploi. Notons dans ce contexte que la Recommandation emploi mentionne le traitement de données collectées auprès de tiers alors que la présente contribution reprend l'analyse du PFPDT et qualifie les courtiers en données non pas de tiers, mais de sous-traitants.

944 On pensera à l'exemple cité en guise d'introduction ; ROUVROY quant à elle cite une étude de *Deloitte* qui a pu montrer que l'analyse des paniers d'achat au supermarché pouvait déterminer l'état de santé du client aussi précisément qu'un médecin dans le cadre d'une consultation médicale, voir ROUVROY, p. 27.

945 Art. 9.2 et 9.3 Recommandation emploi.

du candidat[946]. Dès lors, cette disposition semble être un indice supplémentaire selon lequel le profilage effectué dans le cadre d'une procédure d'embauche devrait être encadré plus strictement, p. ex. en prévoyant qu'il ne peut qu'être effectué par des personnes soumises à une obligation spécifique de secret.

D. Conclusion intermédiaire

Il découle des développements ci-dessus que si la Cour EDH reste fidèle à sa jurisprudence et continue de déterminer le champ de protection de l'art. 8 al. 1er CEDH en fonction de la Convention 108 révisée, la protection des candidats soumis au profilage ne semble que légèrement renforcée par rapport à celle qui prévaut en droit suisse. En effet, contrairement à ce que prévoit le régime suisse, tout traitement de données doit pouvoir se fonder sur un des motifs justificatifs prévus à l'art. 5 al. 2 Convention 108+. De plus, les droits des personnes sont plus généreux en vertu de l'art. 9 Convention 108+ que ce qui a pu être prévu par le Législateur suisse (art. 9 Convention 108+, respectivement les art. 21, 25-26 et 32 LPD). Cette constatation n'a rien de surprenant étant donné que la révision de la LPD a été considérablement influencée par les travaux de révision de la Convention 108.

Si, en revanche, la Cour EDH ne se contente pas de fonder son éventuel raisonnement futur sur la Convention 108+, mais décide de s'inspirer de la Recommandation profilage 2021, la protection des droits des candidats pourrait alors être renforcée au niveau du Conseil de l'Europe. On pensera notamment à la consécration éventuelle d'une définition plus large du profilage, à l'extension du principe d'exactitude aux données anonymes, à l'obligation de fonder tout profilage sur un motif justificatif et non seulement ceux qui seraient contraires à un principe général (sur ce point, la Recommandation profilage 2021 reprend l'approche de la Convention 108+), à un régime plus strict prévoyant notamment un renversement du fardeau de la preuve lorsque le responsable du traitement justifie le profilage sur la base du consentement de la personne concernée et à une interdiction partielle, voire totale du profilage dans certains contextes particulièrement sensibles. On retiendra cependant que même dans cette hypothèse « idéale », certains droits des candidats risquent de ne pas être garantis en pratique. Dans ce contexte, on pensera avant tout au droit d'information renforcé ainsi qu'au droit de s'opposer à un profilage.

Cela étant, les juges de la Cour EDH restent bien évidemment libres de consacrer un régime plus strict, voire plus nuancé que celui proposé par l'une ou l'autre recommandation dans la mesure où il s'agit d'instruments non-contraignants.

946 Art. 19.1 Recommandation emploi.

Il ne fait aucun doute que le RGPD s'applique entre privés. Ainsi, il est plus simple d'engager une procédure sur le fondement du droit de l'UE et d'invoquer, outre le RGPD, le droit fondamental à la protection des données consacré par la Charte des droits fondamentaux de l'UE. Il n'est donc pas étonnant que les ONG particulièrement actives dans ce domaine aient préféré, du moins pour le moment, d'engager des actions en justice sur le fondement du droit européen et non sur la base de la CEDH[947]. Ainsi, on peut se demander si le RGPD et la Charte prévoient un régime plus protecteur des droits des candidats. En raison de l'impact éventuel de la jurisprudence de la CJUE sur celle de la Cour EDH et donc indirectement sur celle du Tribunal fédéral[948], il convient de brièvement se pencher sur le cadre « constitutionnel » européen.

Chapitre 13. Digression : Le cadre « constitutionnel » prévu par l'Union européenne

Contrairement à la Suisse et au Conseil de l'Europe, l'UE a expressément consacré un droit fondamental à la protection des données à caractère personnel distinct du droit au respect de la vie privée et familiale[949]. Dès lors, il convient de contextualiser cette spécificité de l'ordre « constitutionnel » européen dans le cadre de quelques remarques préliminaires (A) avant de se pencher sur un éventuel effet horizontal de cette disposition (B) et d'analyser les limites (potentiellement) imposées par cette disposition aux traitements de données effectués par un employeur (C).

A. Quelques remarques préliminaires

L'art. 8 Charte des droits fondamentaux (ci-après « Charte ») consacre le droit fondamental à la protection des données à caractère personnel. Cette consécration d'un droit fondamental à la protection des données à caractère personnel

947 On pensera, à titre d'exemple, aux arrêts CJUE C-362/14 *Schrems I* et CJUE C-311/18 *Schrems II*. Le système européen offre un avantage supplémentaire. En effet, la CJUE peut être saisie sans avoir épuisé les voies de recours internes, notamment sur la base d'un renvoi préjudiciel ce qui permet d'accélérer la prise de décisions.

948 Cet effet indirect de la jurisprudence « constitutionnelle » de la CJUE sur celle du Tribunal fédéral s'ajoute à l'effet plus direct de la jurisprudence en matière du RGPD, notamment en raison de son application potentiellement extraterritoriale, pour une analyse critique du RGPD et de son application extraterritoriale, voir *supra* Méthodologie.

949 L'art. 7 Charte consacre le droit au respect de la vie privée et familiale tandis que l'art. 8 Charte prévoit un droit fondamental à la protection des données à caractère personnel.

distinct du droit fondamental au respect de la vie privée et familiale fait écho à la tendance constatée dans certains États membres, qui ont consacré des dispositions relatives à la protection des données personnelles dans leurs constitutions respectives dès le début des années 2000[950]. Une atteinte à ce droit fondamental peut alors être constatée indépendamment de toute atteinte au droit fondamental au respect de la vie privée et familiale et a donc pour but d'améliorer la protection des droits des citoyens européens. En effet, l'UE estimait qu'une meilleure protection des droits des individus devait passer par la consécration d'un droit fondamental, qui doit être respecté lors de tout traitement de données personnelles et non seulement en présence de traitements de données qui se rapportent à la sphère privée des personnes concernées[951].

Plusieurs développements ont conduit à l'adoption de ce « nouveau »[952] droit fondamental, au même titre que les droits bioéthiques p. ex.[953].

D'abord, on notera une prise de conscience accrue de la nécessité de mieux protéger la personnalité des individus, notamment face aux développements technologiques conduisant à une fragilisation de la séparation entre le privé et le public d'une part et aux mesures sécuritaires mises en place afin de contrer les menaces terroristes d'autre part[954].

Ensuite, ce « nouveau » droit fondamental a pour but de palier au déficit de nombreuses constitutions nationales qui ne contiennent aucune disposition qui viendrait consacrer une protection constitutionnelle de la protection des données[955].

Enfin, l'art. 8 Charte a été introduit dans la mesure où le Législateur européen ne souhaitait pas consacrer un droit fondamental à l'autodétermination en matière informationnelle, qui est un concept d'origine allemande (repris en droit constitutionnel suisse) et qui trouve son fondement dans le droit fondamental à la liberté d'action (*Handlungsfreiheit* en droit allemand)[956]. En effet, l'introduction, dans la Charte, d'un droit à l'autodétermination en matière

950 EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, p. 88.

951 KOKOTT/SOBOTTA, pp. 223 et 225.

952 On rappellera que le contenu de ce droit n'est pas nouveau, ce que laisse entendre le renvoi à l'art. 8 CEDH dans les Explications relatives à la Charte, voir STREINZ/MICHL, p. 385.

953 RIESZ, art. 8 Charte, N 23 ; STREINZ/MICHL, p. 385.

954 RIESZ, art. 8 Charte, N 23.

955 JOHLEN, art. 8 Charte, N 2 ; à cette époque, l'Allemagne, l'Autriche, le Portugal, l'Espagne ainsi que les Pays-Bas avaient déjà consacré plusieurs dispositions constitutionnelles, qui venaient protéger certains aspects du droit à la protection des données, voir EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, p. 88.

956 BELSER, § 2, N 27 ss.

informationnelle a été discutée, mais rejetée[957]. En d'autres termes, l'introduction de ce droit fondamental distinct du droit au respect de la vie privée et familiale garanti à l'art. 7 Charte avait également pour but de consacrer un système de « checks and balances » en matière de protection des données plutôt que ce droit abstrait d'origine allemande, qui implique, en son essence, que le consentement de la personne concernée est requis pour tout traitement de données envisagé[958].

L'art. 8 Charte a acquis valeur contraignante avec l'entrée en vigueur du Traité de Lisbonne qui lui octroie la même portée qu'aux traités fondateurs de l'UE : le Traité sur l'Union européenne (ci-après « TUE ») et le Traité sur le fonctionnement de l'Union européenne (ci-après « TFUE »). Avant l'entrée en vigueur du Traité de Lisbonne, la protection des données était déjà garantie dans les États membres par le biais de la jurisprudence de la Cour EDH dans la mesure où tous les États membres de l'UE ont également ratifié la CEDH. Si l'art. 8 Charte reprend la structure de la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[959] (ci-après « DPD ») (désormais remplacée par le RGPD), cette disposition se fonde en outre sur la jurisprudence de la Cour EDH relative à l'art. 8 CEDH, la Convention 108, les traditions constitutionnelles des États membres de l'UE, l'art. 17 Pacte ONU-II, la DUDH ainsi que les Lignes directrices de l'OCDE[960]. Les divers fondements de cette disposition influencent la CJUE dans l'interprétation de cette disposition.

Malgré ces précisions, le fondement normatif de l'art. 8 Charte reste peu clair[961]. Sans avancer ni une quelconque définition ni une jurisprudence pertinente de la CJUE, WOLFF estime que l'art. 8 Charte est la seule source d'un droit

957 RIESZ, art. 8 Charte, N 2 s. ; dans le même sens, mais moins explicite, voir JOHLEN, art. 8 Charte, N 5 ou KNECHT, art. 8 Charte, N 2.

958 KRANENBORG, art. 8 Charte, N 08.23 ss.

959 Pour un résumé des développements qui ont conduit à l'adoption de la Directive 96/46/CE, voir EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, pp. 82 ss.

960 Explication ad article 8 – Protection des données à caractère personnel, Explications relatives à la Charte des droits fondamentaux (2007/C 303/02) du 14 décembre 2007 ; par rapport à la CEDH, on rappellera que dans la mesure où la Charte contient des droits correspondant à des droits garantis par la CEDH, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention (art. 52 al. 3 Charte) ; pour des exemples d'arrêts dans lesquels la CJUE fait explicitement référence à la CEDH, voir KOKOTT/SOBOTTA, p. 223 ; cela étant, on notera que s'il est vrai que la Cour EDH a certes considérablement développé le droit de la protection des données, elle a coutume de laisser une marge de manœuvre plus importante aux États que la CJUE, notamment en matière de traitements effectués dans le but de protéger la sécurité nationale, voir FABBRINI, pp. 19 s.

961 LOCK, art. 8 Charte, N 4.

à l'autodétermination en matière informationnelle[962]. STREINZ semble partager l'analyse de WOLFF, mais reste plus réservé dans la mesure où il précise que sans le nommer expressément, la CJUE aurait consacré certains aspects d'un droit fondamental à l'autodétermination en matière informationnelle[963]. AUGSBERG quant à lui fait valoir que l'art. 8 Charte consacre le droit fondamental de déterminer de manière autonome si et quelles données personnelles peuvent être publiées et à quelles fins elles peuvent être traitées. On notera que cet auteur ne mentionne pas un droit à l'autodétermination en matière informationnelle bien qu'une certaine idée d'un droit à contrôler les traitements effectués sur la base des données personnelles semble transparaître dans son commentaire[964]. LOCK estime que cette disposition consacre « probablement » un contrôle sur les données à caractère personnel. Ce droit à un certain contrôle sur les données personnelles serait même la valeur ajoutée de l'art. 8 Charte par rapport à la protection offerte par l'art. 7 Charte. Cet auteur relève toutefois que ce droit consacré à l'art. 8 Charte va moins loin que le droit à l'autodétermination en matière informationnelle tel que conçu par certaines juridictions constitutionnelles nationales[965]. KOKOTT et SOBOTTA estiment que la valeur ajoutée de cette disposition tient au fait qu'elle couvre tous les traitements de données personnelles et non seulement les traitements de données personnelles qui relèvent de la sphère privée[966]. D'autres auteurs ne s'attardent pas même sur cette question[967].

Si ces différentes positions révèlent la difficulté de circonscrire le droit fondamental à la protection des données, l'absence d'une analyse doctrinale claire a l'avantage de laisser plus de flexibilité à la CJUE lorsqu'elle est appelée à trancher de nouvelles questions[968]. Au vu de la genèse de la disposition, de sa lettre et de la jurisprudence récente de la CJUE, il semble difficilement

962 WOLFF, art. 8 Charte, N 3.

963 STREINZ, art. 8 Charte, N 4. Il estime, en effet, que le droit fondamental consacré à l'art. 8 Charte constitue un aspect du droit fondamental au respect de la sphère privée. Ainsi, sa position rejoint celle qui prévaut en droit constitutionnel suisse, voir *supra* Chapitre 11. Le cadre constitutionnel suisse ; on notera que cet auteur semble avoir nuancé son analyse. En effet, quelques années plus tôt, dans un article publié en 2011, STREINZ estimait que l'art. 8 al. 1er Charte protégeait un pouvoir décisionnel autonome par rapport à l'utilisation qui est faite des données personnelles (*Art. 8 I GRCh schützt nämlich die 'autonome Entscheidungsgewalt' über die eigenen Daten*), voir STREINZ/MICHL, p. 385.

964 AUGSBERG, art. 8 Charte, N 6.

965 LOCK, art. 8 Charte, N 4.

966 KOKOTT/SOBOTTA, pp. 223 et 225.

967 FOLZ, art. 8 Charte, N 1 ss.

968 À ce sujet, STREINZ et MICHL précisent que l'art. 8 Charte pourrait avant tout gagner en importance lorsqu'il s'agit de contrer des développements indésirables sur le lieu de travail, voir STREINZ/MICHL, p. 388.

concevable d'admettre l'existence, en droit constitutionnel européen, d'un véritable droit à l'autodétermination en matière informationnelle. Cela étant, sur la base des développements susmentionnés, l'art. 8 Charte semble consacrer un degré minimal de contrôle sur les traitements de données personnelles.

B. La portée de l'art. 8 Charte entre particuliers

Contrairement à ce que pourrait laisser entendre la lettre de l'art. 8 al. 1er Charte, cette disposition consacre d'abord une obligation négative[969]. En raison de sa lettre et à la lumière de l'art. 16 TFUE, l'art. 8 Charte vient toutefois également protéger des droits plus complexes, notamment sous forme d'obligations positives[970]. Les obligations positives peuvent découler de la jurisprudence de la Cour EDH ou être jugées nécessaires à la suite de l'avènement de nouvelles formes de traitements de données[971]. Ces obligations positives imposent la mise en place d'un cadre juridique efficace en matière de protection des données[972]. La reconnaissance d'obligations positives permet ainsi de consacrer, en droit européen, des réponses à de nouvelles questions complexes et relèvent donc d'une grande importance[973], même si l'étendue de ces obligations positives reste à être précisée[974]. En bref, les particuliers peuvent être liés par les dispositions qui découlent de l'art. 8 Charte lorsque l'UE ou les États membres adoptent des dispositions applicables entre particuliers en vertu de leurs obligations positives, comme p. ex. le RGPD, ou si le pouvoir judiciaire accordait des effets horizontaux à cette disposition[975].

S'il est avéré que l'art. 8 Charte peut imposer le respect de certaines obligations positives aux autorités compétentes, il convient de se demander si cette disposition peut également déployer des effets directement entre particuliers.

---

969 Dans ce contexte, STREINZ et MICHEL précisent que cette disposition consacre « des obligations négatives traditionnelles » (*klassisches Abwehrrecht gegen den Staat*), voir STREINZ/MICHL, p. 385.

970 AUGSBERG, art. 8 Charte, N 8 ; KNECHT, art. 8 Charte, N 4 ; MARSCH, p. 249.

971 KNECHT, art. 8 Charte, N 4.

972 AUGSBERG, art. 8 Charte, N 9 ; MARSCH, pp. 249 s.

973 STREINZ, art. 8 Charte, N 6 et 14.

974 MARSCH, pp. 265 ss.

975 Bien que plus loin dans leur contribution, KOKOTT et SOBOTTA estiment que l'art. 8 Charte ne déploie pas d'effets horizontaux directs, ils précisent au sujet du respect des obligations positives face aux traitements de données effectués par des particuliers qu' « [traduction] en principe, la reconnaissance d'un effet horizontal direct du droit de la protection des données peut être justifié comme un moyen [parmi d'autres] de respecter ces obligations positives (*in principle horizontal obligations under data protection law can be justified as a way to discharge these positive obligations*)», voir KOKOTT/SOBOTTA, p. 226.

La portée entre particuliers de l'art. 8 Charte se déterminera en vertu de l'art. 51 al. 1er Charte[976], qui fixe que les droits consacrés par la Charte s'adressent aux institutions et organes de l'UE ainsi qu'aux États membres lorsqu'ils mettent en œuvre le droit européen. Ainsi, en vertu de cette disposition, l'art. 8 Charte ne s'adresse pas aux particuliers et ne déploie dès lors pas d'effets horizontaux directs. La CJUE semble confirmer cette lecture dans la mesure où elle n'a pas explicitement reconnu un effet horizontal direct à l'art. 8 Charte[977]. Une telle lecture n'est d'ailleurs proposée que par une minorité en doctrine[978]. À ce titre, AUGSBERG rappelle que la lettre de l'art. 51 al. 1er première phrase semble plutôt contraire à une telle lecture[979]. FOLZ va même plus loin en précisant que la reconnaissance d'un effet horizontal direct à l'art. 8 Charte est exclu[980], même si cela peut étonner au vu des risques maintes fois évoqués qui sont engendrés par les nouveaux traitements de données effectués par des particuliers[981]. De surcroît, MARSCH rappelle que les affaires qui ont conduit la CJUE à reconnaître un effet horizontal direct à certains droits consacrés dans la Charte soulevaient toutes des questions relatives au principe d'égalité ou à l'interdiction de discrimination et non à l'une des libertés « classiques ». Selon cet auteur, une extension de cette jurisprudence aux autres droits consacrés dans la Charte semble dès lors peu probable[982].

Cela étant, l'art. 51 al. 1er Charte précise, d'une part, que les États membres sont liés par les droits consacrés dans la Charte uniquement lorsqu'ils contribuent à la mise en œuvre du droit européen. D'autre part, cette disposition fixe

976 STREINZ/MICHL, p. 385.

977 Après une analyse approfondie des conclusions de l'Avocat général KOKOTT dans l'affaire *Promusicae* et de l'affaire *Google Spain*, MARSCH estime que ces deux affaires peuvent être lues comme de premiers indices selon lesquels la CJUE pourrait se diriger vers la consécration d'un effet horizontal direct de l'art. 8 Charte, voir MARSCH, pp. 252 ss. ; pour une lecture similaire, mais moins critique de l'affaire *Google Spain*, voir FABBRINI, pp. 16 s. et 21. On notera que cet auteur est d'avis que ce développement vers une telle consécration est, entre autres, dû au contexte institutionnel de l'époque, voir idem, pp. 18 s. ; dans son article publié lorsque l'affaire *Google Spain* était encore pendante devant la CJUE, KOKOTT elle-même affirme que l'art. 8 Charte n'a pas vocation à trouver application entre particuliers, mais uniquement à influencer l'interprétation de la DPD (en vigueur au moment du litige), voir KOKOTT/SOBOTTA, p. 227.

978 Pour un aperçu de cette doctrine minoritaire, voir MARSCH, p. 248.

979 AUGSBERG, art. 8 Charte, N 9 ; dans le même sens, voir MARSCH, p. 248 et KOKOTT/SOBOTTA, p. 225.

980 FOLZ, art. 51 Charte, N 10 et 11 ; dans le même sens, voir STREINZ, art. 8 Charte, N 6.

981 À titre d'exemple, voir MARSCH, p. 247, STREINZ/MICHL, p. 385 ou KOKOTT/SOBOTTA, p. 226.

982 MARSCH, pp. 248 s. ; cet auteur relativise sa position quelques pages plus loin, voir idem, pp. 252 ss.

que la Charte s'adresse aux institutions et organes de l'UE dans le respect du principe de subsidiarité. En bref, si cette disposition semble exclure un effet horizontal direct de l'art. 8 Charte, elle n'exclut pas (au contraire) un effet horizontal indirect du droit fondamental à la protection des données à caractère personnel. Au vu de ces quelques développements, on retiendra que ce droit fondamental déploie des effets entres particuliers à travers une interprétation du droit secondaire à la lumière de la Charte[983]. En de termes plus concrets, le RGPD doit être interprété à la lumière de l'art. 8 Charte[984]. On notera que le contrôle de la CJUE quant à savoir si l'application du RGPD dans un contexte donné respecte les droits prévus à l'art. 8 Charte a été qualifié, à juste titre, d'« intense »[985]. En matière de protection des données, les États membres ne jouissent pas de la même marge de manœuvre que dans d'autres domaines juridiques[986]. L'inverse n'est pourtant pas pertinent dans la mesure où l'art. 8 Charte doit être interprété de manière autonome, c'est-à-dire sans prendre en compte le droit secondaire (sauf si les juges compétents procèdent à une interprétation historique[987]).

Brièvement, on rappellera que les droits fondamentaux consacrés dans la Charte peuvent également déployer certains effets entre particuliers lorsqu'est en cause une des quatre libertés du marché commun. STREINZ et MICHL relèvent à juste titre que de telles constellations risquent d'être particulièrement fréquentes dans le cadre de l'emploi, notamment si un employeur décide de s'établir dans un autre État membre et enfreindrait, ce faisant, les droits des candidats consacrés à l'art. 8 Charte dans l'État membre d'accueil, p. ex. à la suite d'un traitement de données effectué dans le cadre de la procédure d'embauche. Inversement, un candidat peut décider de postuler dans un autre État membre et s'opposer à un traitement de données effectués dans le cadre de

983 WOLFF, art. 8 Charte, N 4 ; MARSCH, p. 250.

984 LOCK, art. 8 Charte, N 5 ; dans le même sens, voir WOLFF, art. 8 Charte, N 16 ; pour une analyse critique de cet effet horizontal indirect de l'art. 8 Charte, voir MARSCH, pp. 251 s.

985 STREINZ, art. 8 Charte, N 12.

986 Pour trois exemples qui reflètent ce contrôle « intense » de la CJUE en matière de protection des données (déjà connu sous le régime précédant l'entrée en vigueur du RGPD), voir STREINZ, art. 8 Charte, N 13 s.

987 WOLFF, art. 8 Charte, N 4 ; dans le même sens, voir FOLZ, art. 8 Charte, N 2 ; MARSCH quant à lui précise que le droit secondaire ne devrait être utilisé en tant que source d'inspiration uniquement lorsqu'il s'agit d'interpréter l'art. 8 Charte dans une relation verticale. Les règles de droit secondaire mises en place par le pouvoir législatif, qui sont le fruit de diverses décisions politiques, ne sauraient être déterminantes lorsque le pouvoir judiciaire est appelé à interpréter l'art. 8 Charte dans la mesure où une interprétation de l'art. 8 Charte à la lumière du droit secondaire porterait atteinte au pouvoir discrétionnaire dont dispose le pouvoir législatif lorsqu'il adopte (voire modifie) le droit secondaire en vertu de son obligation positive, voir MARSCH, p. 259.

cette procédure d'embauche à l'étranger. Dans ces hypothèses, la portée de l'art. 8 Charte dépendra avant tout de savoir si les juges compétents adoptent une approche généreuse du caractère transfrontalier du litige[988]. En effet, si une telle approche est privilégiée, elle permet au juge de régler le litige sur le seul fondement du droit européen et par conséquent de consacrer une portée plus importante à l'art. 8 Charte à travers l'Europe[989].

Si la consécration de l'art. 8 Charte a eu pour conséquence d'élever certaines dispositions du droit secondaire en droit constitutionnel et que la CJUE a, sur ce fondement, procédé à des interprétations généreuses de la DPD[990], force est de constater que comme en droit suisse ou dans la jurisprudence de la Cour EDH, cette disposition ne déploie pas d'effets directs entre particuliers.

Après avoir déterminé la portée de l'art. 8 Charte entre particuliers, comme p. ex. un employeur et un candidat, encore faut-il déterminer si les droits consacrés à l'art. 8 al. 2 Charte sont respectés lorsqu'un employeur effectue un profilage d'un candidat.

C. Le contenu du droit à la protection des données à caractère personnel

Au-delà du « droit de toute personne à la protection des données à caractère personnel la concernant » prévu à l'art. 8 al. 1er Charte dont les contours restent peu clairs, l'art. 8 al. 2 Charte a érigé quatre principes consacrés dans la DPD en droit primaire. Il s'agit du principe de finalité, du principe de la bonne foi, du principe du consentement et le droit d'accès aux données personnelles[991]. En guise de rappel, on notera que le respect de ces principes n'exclut pas que l'art. 7 Charte, qui consacre le droit au respect de la vie privée et familiale, puisse

988 Pour des précisions quant au rôle de la CJUE, qui est particulièrement important dans les affaires qui soulèvent de nouvelles questions en droit de la protection des données, voir FABBRINI, p. 22.

989 STREINZ/MICHL, pp. 387 s.

990 Pour une analyse critique de la jurisprudence *Google Spain*, qui a conduit à la consécration d'un droit à l'oubli sur le fondement de la DPD et la Charte, voir FABBRINI, pp. 20 s. À juste titre, cet auteur soulève d'une part les problèmes de mise en œuvre de cette jurisprudence généreuse et d'autre part, il précise qu'elle crée de nouveaux conflits de droits fondamentaux que la CJUE semble résoudre en consacrant une hiérarchie presque absolue en plaçant le droit à la protection des données à caractère personnel « au sommet de cette pyramide ». Or, cette tendance pourrait nuire *in fine* à la protection des droits fondamentaux en général, comme p. ex. à la liberté d'expression ou à la liberté d'entreprendre.

991 STREINZ, art. 8 Charte, N 9.

être violé[992]. Si une analyse de la portée de l'art. 7 Charte ne fait pas l'objet de la présente contribution, il semble cependant particulièrement important de brièvement clarifier ce qui doit être entendu par un traitement de bonne foi et le principe de finalité.

Si le contenu du principe de la bonne foi n'a jamais été clarifié, WOLFF estime que le respect de ce principe implique que tout traitement doit être prévisible et transparent. La prévisibilité d'un traitement implique que le traitement envisagé soit effectué dans le cadre de ce qui pouvait être légitimement attendu par la personne concernée. Le critère de la transparence quant à lui exige que la personne concernée soit informée à propos des traitements envisagés au moment de la collecte de ses données. Ainsi, à défaut d'une définition claire du principe de la bonne foi, le respect des droits procéduraux (avant tout lors de la collecte des données) est souvent considéré être un moyen de respecter ce principe[993].

Le respect du principe de finalité quant à lui implique que la finalité du traitement de données doit être communiquée à la personne concernée en amont du traitement envisagé et que le traitement qui s'ensuit doit s'effectuer à la lumière de la finalité ainsi communiquée. Ce principe a pour but premier de limiter l'étendue des traitements possibles[994]. Or, comme nous l'avons vu plus haut déjà, le profilage est souvent effectué à l'insu de la personne concernée et se fonde sur des évaluations qui sont peu prévisibles. Ce traitement de données ne permet donc pas, notamment en raison de son mode opérationnel, d'être utilisé de manière prévisible et transparente au sens de l'art. 8 al. 2 Charte. De même, ce mode opérationnel ne permet ni de déterminer la finalité précise du traitement lors de la collecte des données ni (ou que très difficilement) de limiter les nouvelles connaissances qui découlent du traitement.

Enfin, on rappellera qu'une des conditions d'un consentement valide consiste en sa nature volontaire. Comme le précise WOLFF à juste titre, la nature volontaire d'un consentement peut être remise en cause dans un rapport asymétrique[995], comme p. ex. dans le rapport entre un employeur et un employé.

992 À ce sujet, KOKOTT et SOBOTTA rappellent, à juste titre, que si les principes de la bonne foi et de la finalité ainsi que le consentement de la personne concernée (ou un autre motif justificatif prévu par la loi) sont respectés, un traitement de données ne portera pas atteinte à l'art. 8 Charte. Or, la collecte, l'enregistrement ou le transfert des données traitées peuvent porter atteinte au droit consacré à l'art. 7 Charte et donc nécessiter une justification. Ces constellations devraient toutefois être plutôt rares en pratique, voir KOKOTT/SOBOTTA, p. 226.

993 WOLFF, art. 8 Charte, N 34 ss.

994 WOLFF, art. 8 Charte, N 37 ss.

995 WOLFF, art. 8 Charte, N 30.

Le RGPD précise les limites possibles au droit fondamental à la protection des données, qui sont consacrées à l'art. 8 al. 2 Charte. Ces limites doivent toutefois être compatibles avec l'art. 8 al. 2 première phrase ainsi que l'art. 52 al. 1er Charte[996]. Comme nous l'avons vu plus haut, le RGPD n'offre qu'une protection partielle des droits des candidats soumis au profilage. Dans ce contexte, on pourrait imaginer un renvoi préjudiciel qui chercherait à savoir si le RGPD est conforme à l'art. 8 Charte, du moins dans quelques constellations bien précises[997]. On pourrait alors de demander si la CJUE devrait reconnaître, dans l'hypothèse d'un profilage effectué lors d'une procédure d'embauche, que l'UE a failli à ses obligations positives. WOLFF est d'avis que l'UE viole ses obligations positives lorsqu'aucune mesure législative est mise en place ou lorsque les mesures existantes sont insuffisantes. Dans la mesure où le RGPD impose que tout traitement effectué doit pouvoir se fonder sur une des conditions fixées à l'art. 6 RGPD, WOLFF estime que la mise en place de cette mesure serait suffisante à respecter les obligations positives qui découlent de l'art. 8 Charte[998]. Reste à savoir si la CJUE partagerait cette analyse.

À la lumière de ces développements, on rappellera que le droit suisse n'impose pas que tout traitement de données puisse se fonder sur un motif justificatif (principe du *opt-in* consacré en droit européen). En d'autres termes, le Législateur suisse ne semble donc pas avoir consacré un régime qui respecte les obligations positives découlant de la Charte ce qui pourrait impacter la décision d'adéquation de l'UE[999]. Toutefois, comme nous l'avons vu plus haut, l'implémentation du principe du *opt-in* à lui seul ne suffit pas à garantir un degré suffisant de contrôle au candidat dans l'hypothèse où un employeur effectue un profilage. En effet, peu nombreux sont les responsables de traitement qui prennent le soin de fonder le traitement sur un motif justificatif, notamment en raison de la nature souvent secrète de cette forme de traitement de données. Dans le cas particulier de traitements de données affectant l'accès au marché

996 STREINZ, art. 8 Charte, N 1.

997 Dans ce contexte, on pensera aux affaires *Digital Rights Ireland Ltd* et *Kärntner Landesregierung* qui ont conduit la CJUE à constater que la Directive 2006/24/CE sur la conservation des données violait les art. 7 et 8 Charte ; pour une analyse de cette jurisprudence, voir FABBRINI, pp. 12 ss.

998 WOLFF, art. 8 Charte, N 20. S'il est vrai que WOLFF se réfère à la DPD, il ne fait aucun doute que son argumentation vaut également à la lumière du RGPD dans la mesure où le RGPD a repris ce principe, également connu en droit du Conseil de l'Europe, mais non-implémenté en droit suisse ; dans une veine plus générale, MARSCH estime que l'adoption de la DPD qui trouve également application entre privés conduit au respect de cette obligation, voir MARSCH, p. 250.

999 Dans le même sens (et pour une analyse approfondie des autres critères qui risquent d'impacter cette décision d'adéquation), voir MÖHLE, pp. 599 ss., mais surtout p. 601.

du travail, il est à espérer qu'un tribunal définisse les obligations positives découlant de l'art. 8 Charte plus généreusement que ce qui a été suggéré en doctrine.

Enfin, on rappellera que l'art. 8 Charte déploie potentiellement un effet (horizontal indirect) extraterritorial et a donc le potentiel de trouver application entre deux particuliers suisses également[1000]. En effet, en vertu du chapitre VI RGPD, un transfert de données vers un État tiers ne peut qu'être effectué si l'État tiers garantit une protection adéquate des données personnelles transférées. Ainsi, le droit de l'État tiers doit offrir une protection équivalente à celle prévue en droit de l'UE, qui englobe les garanties découlant de l'art. 8 Charte.

D. Conclusion intermédiaire

En guise de conclusion de ce chapitre, il convient de retenir les cinq points suivants :

— spécificité du droit « constitutionnel » européen, l'art. 8 Charte, qui consacre un droit fondamental à la protection des données à caractère personnel distinct du droit au respect de la vie privée et familiale (art. 7 Charte) a donc un champ de protection plus large que celui de l'art. 7 Charte, qui n'englobe « uniquement » les traitements de données qui se rapportent à la sphère privée. Toutefois, contrairement à ce qui a pu être prévu en droit constitutionnel suisse, la Charte ne garantit pas un droit à l'autodétermination en matière informationnelle, mais consacre quatre principes essentiels, qui trouveront application chaque fois qu'une institution ou un organe de l'UE procède à un traitement de données à caractère personnel (ou qu'un État membre de l'UE met en œuvre le droit européen) ;

— si cette disposition consacre avant tout des obligations négatives, plusieurs obligations positives peuvent en découler. Les contours précis de ces obligations positives doivent toutefois encore être précisés par la CJUE. Le souci de respecter (une partie) de ces obligations a, entre autres, conduit à l'adoption du RGPD, qui s'applique également entre particuliers. Reste à savoir si l'adoption de ce règlement constitue une mesure suffisante afin de respecter ces obligations positives, notamment dans les relations de travail ;

— dans ce contexte, on peut se demander si les autorités compétentes devraient accorder un effet horizontal direct à l'art. 8 Charte. La jurisprudence pertinente de la CJUE peut être lue comme un indice que la consécration explicite d'un tel effet pourrait être envisagée dans le futur. Toutefois, cette

1000 LOCK, art. 8 Charte, N 17 ; pour une analyse de cette question soulevée devant la CJUE dans l'affaire *Google Spain*, voir FABBRINI, pp. 15 s. ; par rapport à la question épineuse de l'effet extraterritorial du RGPD, voir *supra* Méthodologie.

même jurisprudence illustre à quel point une telle consécration soulèverait de nombreux nouveaux problèmes ;

— si l'effet horizontal direct semble exclu (pour l'instant), il ne fait aucun doute que l'art. 8 Charte déploie des effets horizontaux indirects, notamment dans les hypothèses où le pouvoir judiciaire est appelé à interpréter le RGPD ou dans les constellations mettant en cause une des quatre libertés du marché commun *et* les droits protégés par l'art. 8 Charte ;
— le potentiel de cette disposition reste à être exploré. La jurisprudence de la CJUE, qui est l'autorité la plus influente en matière de protection des données, n'en est qu'à ses débuts. Tant le Tribunal fédéral que la Cour EDH devront donc suivre les développements de cette jurisprudence avec beaucoup d'attention lorsqu'ils seront appelés à dessiner les (nouveaux) contours de l'art. 13 al. 2 Cst. et de l'art. 8 CEDH respectivement.

Chapitre 14. Conclusion de la troisième partie

La deuxième partie de cette contribution a pu montrer que les lois fédérales actuellement en vigueur n'étaient pas aptes à protéger les droits des candidats de manière efficace. Cette troisième partie avait pour but de savoir dans quelle mesure le cadre constitutionnel imposait la prise de mesures allant au-delà du dispositif fédéral en vigueur. En guise de conclusion de cette troisième partie, on retiendra les trois points suivants :

L'art. 13 al. 2 Cst. consacre un droit à l'autodétermination en matière informationnelle soit « le droit de ne pas accepter un traitement qui ne correspond pas à la volonté exprimée [de la personne concernée] »[1001]. Ce droit fondamental impose le respect d'obligations tant négatives que positives, comme p. ex. l'obligation de garantir le respect des droits d'accès, d'effacer les données traitées de manière illicite ou de faire corriger les données erronées. Dans le cas précis d'un profilage effectué lors d'une procédure d'embauche, on a pu montrer que des obligations positives allant au-delà de celles qui sont généralement admises semblent s'imposer. La constatation de l'existence d'une obligation positive peut alors entraîner diverses conséquences. Dans le cadre de cette troisième partie, plusieurs modifications législatives ont été analysées ainsi que la nécessité de procéder à une interprétation conforme de certaines notions vagues à la lumière de l'art. 13 al. 2 Cst. La reconnaissance d'un effet horizontal direct de cette disposition a été discutée, mais finalement rejetée dans la mesure où il n'est que

1001 MEIER, Protection des données, N 17.

très peu probable que la reconnaissance d'un tel effet contribue à améliorer la protection des droits des candidats. En bref, le cadre constitutionnel suisse semble imposer la prise de mesures tant sur le plan législatif que judiciaire.

Au vu de l'impact de la jurisprudence de la Cour EDH sur le droit suisse, une analyse de cette jurisprudence s'imposait dans le cadre de cette contribution. S'il est vrai que la Cour EDH a considérablement contribué au développement du droit de la protection des données en Europe, la jurisprudence relative aux nouveaux traitements de données est (presque) inexistante. Les juges de Strasbourg n'ont ni défini le profilage (ou la décision individuelle automatisée) ni précisé les contours d'un éventuel régime renforcé de ces nouveaux traitements de données. Cela étant, les travaux d'autres organes du Conseil de l'Europe, notamment ceux du Comité des Ministres, ont eu et ont toujours un caractère pionnier en matière de protection des données. Les innovations juridiques au niveau du Conseil de l'Europe passeront donc probablement par le biais d'une application jurisprudentielle du régime (incomplet) de la Convention 108 révisée et de la Recommandation profilage modifiée en novembre 2021 (en moindre mesure). Même si ce dernier dispositif n'est pas contraignant, la Cour EDH s'est déjà appuyée sur d'autres Recommandations lorsqu'elle était amenée à trancher de nouveaux litiges. Cela étant, s'il est certain que cette Recommandation apporte quelques précisions importantes (harmonisation de la définition du profilage), il n'est pas certain que le régime proposé offre une protection satisfaisante des droits des candidats.

Spécificité du droit « constitutionnel » européen, la Charte consacre un droit fondamental à la protection des données à caractère personnel distinct du droit au respect de la sphère privée et familiale. Le champ de protection de ce droit fondamental a l'avantage d'être plus large que celui du droit fondamental au respect de la sphère privée et familiale dans la mesure où il couvre *tous* les traitements de données personnelles et non seulement ceux qui relèvent de la sphère privée. Si une telle extension explicite de la protection constitutionnelle des droits des personnes concernées est à saluer, on rappellera toutefois que de nombreux traitements de données problématiques peuvent également porter sur des données non-personnelles et ne seront dès lors pas couverts par cette disposition. Cela étant, il est incontestable que cette disposition impose le respect d'obligations tant négatives que positives. Si la CJUE a tendance à reconnaître l'existence d'obligations positives de manière assez généreuse, elle n'a pas reconnu un effet horizontal direct à cette disposition. Toutefois, il n'est pas exclu qu'elle procède à la consécration d'un tel effet dans le futur, même si cela impliquerait de clarifier de nombreuses questions le cas échéant et qu'il n'est pas certain qu'une telle portée de cette disposition entre particuliers améliore effectivement la protection des droits des candidats au sein de l'UE.

Résumé des propositions

Plusieurs lacunes quant au régime juridique qui encadre le profilage effectué lors d'une procédure d'embauche ont pu être identifiées tout au long de cette contribution. Au vu des développements considérables des traitements de données offerts par les courtiers en données, une interdiction généralisée de ces traitements consacrée en droit suisse semble illusoire et nuirait, de surcroît, aux utilisations bénéfiques qui peuvent en être faites. Il importe donc de réfléchir à des mesures juridiques qui permettent d'encadrer ces traitements de données de manière efficace sans pour autant nuire au développement des nouvelles technologies. Cela étant, l'accès au marché du travail ne devrait pas être soumis à la condition de renoncer au droit à l'autodétermination en matière informationnelle[1002].

La constatation d'une violation d'une obligation positive par le pouvoir judiciaire peut être accompagnée de directives portant sur une nouvelle réglementation. Indépendamment d'une telle constatation par le pouvoir judiciaire, le pouvoir législatif peut bien évidemment décider de modifier le régime légal en vigueur[1003]. Dans le cadre d'un profilage effectué lors d'une procédure d'embauche, on pensera aux potentielles nouvelles réglementations suivantes :

1. une précision de l'art. 328b CO quant aux traitements de données automatisés licites et quant au principe de transparence qui pourrait englober une obligation explicite de rendre le profilage transparent lors d'une procédure d'embauche, p. ex. dans les offres d'emploi ;
2. une nouvelle définition (plus dynamique) de la « donnée personnelle sensible » qui tiendrait compte de la finalité et des circonstances du traitement ;
3. un droit d'accès renforcé également dans l'hypothèse d'un profilage qui ne serait *pas* suivi d'une décision individuelle automatisée, accompagné d'un renversement du fardeau de la preuve ;
4. l'octroi de compétences supplémentaires au PFPDT ; on pensera notamment à la consécration de la possibilité d'engager une procédure au nom et pour le compte des candidats concernés ;
5. une amélioration de l'indépendance du PFPDT tant sur le plan financier que personnel.

De plus, la constatation de l'existence d'une obligation positive peut exiger une interprétation de normes en vigueur à la lumière des dispositions constitutionnelles pertinentes. Dans ces cas de figure, les dispositions constitutionnelles

1002 Dans le même sens à propos de l'accès au marché du travail aux États-Unis, voir AJUNWA/CRAWFORD/SCHULTZ, p. 776.

1003 Pour une conclusion similaire en droit européen, voir FABBRINI, p. 22.

déploient un effet horizontal indirect. Par le biais de la LPD (et d'autres dispositions fédérales comme p. ex. l'art. 328 CO), l'effet horizontal indirect de l'art. 13 al. 2 Cst. est reconnu de longue date. Plusieurs dispositions floues ont été identifiées dans le cadre de cette contribution. Ainsi, dans le cadre d'un litige opposant un candidat à un employeur, le pouvoir judiciaire sera appelé à interpréter les dispositions suivantes à la lumière de cette disposition constitutionnelle (et, le cas échéant, également à la lumière d'autres dispositions constitutionnelles pertinentes) :

6. le profilage à risque élevé (art. 5 let. g LPD) ;
7. le champ d'application temporel de l'art. 328 CO, notamment face à un traitement automatisé effectué au stade de la procédure d'embauche ;
8. le champ d'application matériel de l'art. 328b CO face au régime plus souple de la LPD ;
9. le droit fondamental en matière informationnelle lui-même, en adoptant une approche plus dynamique que statique prenant également en compte le processus, la finalité et le contexte des traitements de données litigieux.

Enfin, le pouvoir judiciaire pourrait être tenté de développer une règle par substitution, notamment dans les cas où ni une interprétation conforme ni le régime prévu ne parviennent à garantir les droits des candidats. En d'autres termes, on peut se demander si le Tribunal fédéral pourrait développer de nouvelles règles par substitution et ainsi se diriger vers la consécration d'un effet horizontal direct (partiel) de l'art. 13 al. 2 Cst. On rappellera qu'en raison des difficultés de preuve, du (très) faible nombre de recours en matière de protection des données, du défaut de légitimité démocratique des juges et des nombreux traitements de données qui ne soulèvent aucun problème au regard de l'art. 13 al. 2 Cst., la consécration d'un tel effet horizontal direct ne semble pas être une voie à suivre. Cela étant, au vu de la perte de contrôle sur les données personnelles, notamment dans le champ du droit privé, la consécration d'une portée *erga omnes* de ce droit fondamental doit être envisagée. Reste à déterminer si elle devra passer par une codification d'un véritable droit de propriété sur les données qui pourrait également entraîner des conséquences fiscales ouvrant la voie aux autorités publiques de guider les flux de données ou par une limitation du droit d'accumuler des données mise en œuvre par des mesures d'ordre économique.

Les données peuvent être collectées n'importe où dans le monde, à n'importe quel moment, par n'importe qui avant d'être transmises à n'importe quel endroit. Ainsi, la protection des droits des candidats doit impérativement être pensée dans un contexte international. La consécration d'un standard international, du moins de certaines mesures, contribuerait à garantir un niveau

minimal de protection indépendamment du lieu du traitement de données. Les efforts tant au niveau du Conseil de l'Europe que de l'UE vers la consécration d'un droit universel à la protection des données doivent donc être encouragés par la Suisse. En effet, la Suisse en tant que petite nation ne peut que bénéficier d'un régime harmonisé au niveau européen, voire mondial, notamment face à l'avènement de nouveaux traitements de données issus de pays non-démocratiques comme p. ex. la Chine. Au niveau international, on retiendra donc la mesure suivante :

10. L'encouragement des efforts européens à consacrer un droit universel en matière de protection des données[1004].

Les enjeux des nouveaux traitements de données ne peuvent qu'être saisis dans un contexte technologique, économique, social et juridique global. Cette constatation permet de mieux comprendre la complexité des problèmes esquissés et prouve que toute solution devra non seulement considérer la problématique d'un point de vue juridique, mais aussi d'un point de vue économique, social et technologique[1005].

Si la volonté du Législateur d'aborder également la thématique sous un angle technique, voire organisationnel est, en principe, à saluer, force est de constater que les cinq mesures de nature technique prévues par la LPD révisée risquent de ne déployer que peu d'effets en pratique. Ainsi, le cadre juridique prévu devrait être revu en profondeur (laissant les mesures purement techniques de côté, qui devront être proposées par les experts en la matière). On pensera notamment aux mesures suivantes :

11. un encadrement plus strict des codes de conduite dont la portée dans des relations asymétriques reste à être clarifiée ;
12. une réévaluation de la qualification juridique d'une violation de la protection des données dès la conception et par défaut. En effet, une telle violation ne devrait pas être qualifiée de simple violation du devoir de diligence ;

1004 À ce sujet, WALTER précise que « cette coopération [...] doit [...] être mieux institutionnalisée dans nos lois pour permettre notamment aux autorités de partager des informations entre elles, de fournir une assistance mutuelle, de veiller à une application cohérente des dispositions ou de mener des activités de contrôle conjointes et coordonnées », voir WALTER, Perspectives, N 35.

1005 GASSER, pp. 374 s. ; dans son rapport spécifiquement dédié aux risques d'une augmentation importante de profilages effectués sur le lieu de travail (*People Analytics*), *AlgorithmWatch* constate, dans une veine similaire, que ces risques devront être adressés grâce à différents types de solutions. En effet, après examen de 84 lignes directrices en matière d'intelligence artificielle, les auteurs distinguent trois principaux types de solutions consacrées dans ces lignes directrices : des solutions d'ordre technique, des solutions organisationnelles (qui renvoient à la responsabilité des entreprises) et des solutions institutionnelles (qui recouvrent la mise en œuvre de nouvelles lois et une sensibilisation plus importante de la société civile), voir AlgorithmWatch, p. 16.

13. une réévaluation de la fonction des registres des activités de traitement et, le cas échéant, l'abolition de la disposition correspondante ;
14. la consécration d'une obligation de certifier certains traitements de données, comme p. ex. les traitements automatisés effectués dans le cadre d'une procédure d'embauche[1006] ;
15. la consécration explicite d'une obligation d'effectuer une analyse d'impact lorsque le responsable du traitement envisage un profilage dans un domaine sensible, comme p. ex. lorsque le profilage a des effets sur l'accès au marché du travail.

Si la mise en œuvre des diverses mesures susmentionnées par le pouvoir judiciaire d'une part et le pouvoir législatif d'autre part contribuerait certes à une meilleure protection de la personnalité et des droits fondamentaux des candidats, différentes mesures de sensibilisation doivent également être envisagées[1007].

Une meilleure sensibilisation est d'autant plus nécessaire que plusieurs études ont pu montrer que l'opacité de l'économie du numérique a engendré une importante crise de confiance dans la société civile[1008]. Si une telle constatation est certes à déplorer à court terme, elle risque d'avoir des conséquences non-désirées à long terme également. En effet, une crise de confiance importante a le potentiel d'impacter les développements (bénéfiques) de la numérisation[1009]. La notion de « sensibilisation » renvoie à de nombreuses mesures qu'il convient de brièvement esquisser.

En vertu des différentes lois actuellement en vigueur, l'employeur reste responsable du traitement des données du candidat. Ce cadre juridique a pour conséquence que le courtier en données qualifié de sous-traitant est libéré d'une quelconque responsabilité envers le candidat (ce qui n'est pas le cas en droit européen). Cette constatation n'est toutefois pas satisfaisante et soulève, une fois de plus, la question épineuse de savoir sous quelle forme il convient d'encadrer la responsabilité des courtiers en données[1010].

1006 Pour WALTER, cette procédure de contrôle préalable des profilages devrait être menée par le PFPDT, voir WALTER, Perspectives, N 29.

1007 AlgorithmWatch, pp. 41 s.

1008 WEF, p. 3.

1009 Dans son rapport, le WEF cite ROTHENBERG, qui, en 2014 déjà, écrivait que « [traduction] la chaîne d'approvisionnement par laquelle la publicité numérique est créée, diffusée, mesurée et optimisée est si poreuse et périlleuse qu'elle met en péril la confiance des consommateurs et la croissance des entreprises. Le risque est si grave que la capacité d'innovation sous-jacente de l'internet lui-même risque de s'arrêter net », voir WEF, p. 8.

1010 Pour des exemples d'obligations supplémentaires qui pourraient être imposées à des sous-traitants, qui effectuent des profilages de candidats et d'employés pour l'employeur, voir AlgorithmWatch, pp. 39 s.

Une sensibilisation des courtiers en données doit passer par des cours obligatoires au niveau universitaire, qui pourraient aboutir à une forme de serment d'Hippocrate pour ces personnes[1011]. Actuellement, les ingénieurs et les économistes ne suivent cependant pas de cours obligatoires en la matière. Ils apprennent au contraire que plus ils disposent de données, plus leurs analyses automatisées seront précises. Savoir quelle personne physique ou morale devrait être responsable des impacts de ces produits sur les individus *et* la société est laissé aux juristes des entreprises, qui ont alors la tâche compliquée de justifier un traitement (qu'ils ne comprennent guère d'un point de vue technique) qui ne semble pas justifiable[1012]. En bref, la formation universitaire actuelle des futurs courtiers en données ne leur enseigne pas d'anticiper l'impact potentiel des traitements de données développés[1013].

Un tel serment et une telle sensibilisation au niveau universitaire ne suffiront pas à encadrer le profilage de manière efficace. Les employeurs en tant que responsables du traitement doivent ainsi également être sensibilisés à la thématique. Si la sensibilisation des employeurs doit certes passer par une prise de conscience des risques juridiques liés à l'utilisation des nouvelles formes de traitements de données, encore faut-il que les employeurs se rendent compte des risques potentiellement encourus pour leur réputation (risques potentiellement plus grands en raison du faible nombre de procédures engagées). En Suisse, pays des PME, les associations professionnelles semblent être les plus compétentes pour sensibiliser leurs membres à ces risques. À cette fin, elles pourraient p. ex. s'inspirer des Lignes directrices publiées par *AlgorithmWatch* en mai 2021, qui énumèrent 20 aspects que tout employeur souhaitant mettre en place un profilage sur le lieu de travail devrait considérer[1014].

Les candidats potentiellement concernés par un profilage doivent également être sensibilisés à la thématique. Cette sensibilisation de la société civile est nécessaire afin que les personnes visées puissent faire valoir leurs droits (si elles le souhaitent). Elle passe par un engagement accru de diverses institutions.

1011 ZUBOFF, Surveillance Capitalism, p. 255 ; pour une liste possible d'aspects à analyser avant la mise à disposition d'un programme sur le lieu de travail, voir AlgorithmWatch, pp. 40 s.

1012 CHRISTL/SPIEKERMANN, p. 146.

1013 Les seules recommandations allant dans ce sens semblent concerner les algorithmes utilisés soit dans un contexte militaire soit en matière de presse. Or, c'est bien la relation de travail qui se caractérise par le plus grand nombre de traitements de données personnelles effectués entre deux particuliers, voir, pour quelques tentatives d'explications, AlgorithmWatch, p. 40.

1014 AlgorithmWatch, pp. 3 ss.

L'engagement du SECO dont les publications même dépourvues de valeur contraignante sont suivies de près en pratique doit être encouragé. Il en va de même des interventions des inspecteurs cantonaux du travail qui peuvent intervenir au nom et pour le compte d'employés soumis à des mesures de surveillance illicites *pendant* la relation de travail. Il va sans dire que ni le SECO ni les inspecteurs du travail n'ont la compétence d'interférer dans la liberté contractuelle des employeurs au stade de la procédure d'embauche. Une prise de conscience accrue des risques des nouveaux traitements de données pendant la relation de travail pourrait toutefois indirectement influencer le débat autour de l'impact de ces traitements sur l'*accès* au marché du travail.

En tant qu'autorité de surveillance en matière de protection des données, le PFPDT se doit d'intervenir dans le débat public[1015], p. ex. en publiant des prises de position (dépourvues de valeur contraignante[1016], mais très régulièrement consultées par les praticiens), en menant des enquêtes lors de violations signalées de la LPD[1017] ou en informant la société civile à travers la presse[1018]. À titre d'exemple, on rappellera l'engagement du PFPDT dans le cadre de la pandémie du Covid-19[1019] ou sa collaboration avec les enseignants de l'*Agence Kik* en matière de sensibilisation des plus jeunes[1020]. Les précisions quant à la nouvelle définition du profilage n'ont pas encore été publiées, mais auront certes une portée considérable en pratique.

Face aux problématiques de traitements de données effectués dans le cadre des relations de travail, les compétences du SECO d'une part et celles du PFPDT d'autre part ne sont pas toujours faciles à délimiter[1021]. Afin d'éviter

1015 Art. 58 LPD (art. 31 al. 1er aLPD).

1016 Art. 58 al. 1er let. g LPD.

1017 Art. 49 LPD.

1018 À juste titre, MONTAVON précise que « dans ses interventions publiques concernant des affaires particulières, l'autorité de contrôle en matière de protection des données devrait, selon nous, se prononcer uniquement en fait et en droit et renoncer autant que possible à se prononcer en opportunité », voir MONTAVON, p. 721.

1019 À titre d'exemple, on pensera à ses diverses interventions quant aux mesures de sécurité pour les conférences audio et vidéo, aux applications de traçage *Proximity Tracing App* et *SocialPass*, à la plateforme *mesvaccins.ch* ou au certificat, pour un aperçu des communiqués de presse, voir PFPDT, Actualités.

1020 PFPDT, Outils pédagogiques sur la protection des données, 15 juin 2021.

1021 Le SECO peut élaborer des recommandations de bonne pratique relatives à la LTr et ses Ordonnances, le PFPDT par rapport à la LPD. Étant donné que la LTr protège, entre autres, la protection de la santé des employés, que la protection de la santé psychique fait partie intégrante de la protection de la santé telle qu'entendue par la LTr et que la surveillance peut porter atteinte à la santé psychique, toute forme de surveillance sur le lieu de travail porte potentiellement atteinte à la santé des travailleurs concernés (compétence du SECO) et constitue, en même temps, un traitement de données personnelles soumis au contrôle du PFPDT.

des contradictions entre les diverses prises de position, une collaboration étroite entre ces deux entités administratives est essentielle. Une telle collaboration ne doit toutefois pas empêcher le PFPDT (dans sa fonction d'autorité de surveillance) d'intervenir en aval s'il le juge nécessaire, p. ex. s'il estime qu'un employeur s'est certes fondé sur une recommandation du SECO, mais que malgré cela, le traitement de données porte atteinte à la personnalité des personnes concernées. À titre d'exemple, on retiendra la collaboration entre le SECO et le PFPDT lors de la révision de la recommandation du SECO par rapport à l'art. 26 OLT 3, qui interdit la surveillance du comportement sur le lieu de travail.

De surcroît, il est à espérer que les syndicats, forts de leurs expériences dans l'apaisement des relations asymétriques du travail multiplient les efforts de sensibilisation de leurs membres, notamment en matière de nouvelles formes de surveillance sur le lieu de travail[1022]. À titre d'exemple, le plus grand syndicat suisse « UNIA » n'a rien publié à ce sujet sur son site web pourtant très complet sur de nombreux sujets importants pour les employés en Suisse.

Enfin, la sensibilisation de la société civile passe également par la presse. Tous les grands journaux suisses ont, en leur sein, des journalistes qui se sont spécialisés aux questions liées à l'impact des nouvelles technologies. Certains d'entre eux s'expriment de manière fréquente (et critique) sur les réseaux sociaux, à la télévision ainsi que dans la presse écrite et ont ainsi contribué à lancer des procédures d'établissement des faits[1023]. Cette tendance doit impérativement se poursuivre, voire s'accentuer.

Il découle de ces quelques développements qu'une multitude de personnes et d'institutions restent à sensibiliser :

16. les employeurs en tant que responsables du profilage ;
17. les sous-traitants en tant qu'experts en matière de profilage, dont la sensibilisation doit commencer pendant leur formation universitaire ;
18. les syndicats ;
19. l'administration tant fédérale (PFPDT et SECO) que cantonale (inspecteurs du travail) ;
20. la presse.

1022 AlgorithmWatch, p. 47 ; pour une analyse de la situation aux États-Unis, qui retrace le lien entre le déclin des syndicats et l'augmentation significative des mesures de surveillance sur le lieu de travail dès les années 1980, voir AJUNWA/CRAWFORD/SCHULTZ, pp. 740 ss.

1023 À titre d'exemple, voir PFPDT, Rapport final et recommandations du Préposé fédéral à la protection des données et à la transparence (PFDPT) du 4 août 2021 dans le cadre de la procédure d'établissement des faits selon l'art. 29 de la Loi fédérale sur la protection des données du 19 juin 1992 concernant l'application « SocialPass » de SwissHelios Sàrl, à Oberlunkhofen et NewCom4U Sàrl, à Sierre, p. 6.

Enfin et surtout on rappellera que « la réalisation des droits fondamentaux dépend aussi des particuliers eux-mêmes, qu'ils soient des personnes physiques ou des personnes morales. Les autorités jouent certes un rôle capital, mais ne jouissent d'aucun monopole en la matière. Les particuliers définissent les relations qui les lient et sont ainsi en mesure de contribuer de manière importante à rendre les droits fondamentaux effectifs au sein de la société. La réalisation des droits fondamentaux est en somme l'affaire de chaque personne »[1024].

Conclusion

Le droit de la protection des données vise à protéger la personnalité des personnes concernées contre des atteintes de nature abstraite. En sus de leur nature abstraite, ces atteintes aux droits sont, le plus souvent, commises à l'insu de la personne concernée. Dans les (rares) hypothèses où l'individu en cause a connaissance du traitement portant atteinte à ses droits, il n'apprendra l'existence de ce traitement qu'une fois que celui-ci a été effectué. En d'autres termes, l'atteinte aura été commise avant que la personne concernée ait eu la chance d'intervenir, les meilleures mesures restant dès lors les mesures préventives. Or, au vu de la nature abstraite des risques et de la nature secrète de la majorité des traitements de données automatisés, circonscrire les risques en amont s'avère compliqué (et peu gratifiant pour un politicien). En raison de la nature souvent secrète des traitements de données et des voies de recours peu efficaces en pratique, la jurisprudence est (presque) inexistante en la matière et ne contribue donc pas à une meilleure compréhension de ces risques abstraits. La plupart des publications qui portent sur les enjeux potentiels du profilage se contentent de décrire le cadre légal de manière assez, voire trop générale pour constater toujours et encore qu'il est insuffisant[1025]. Or, face à des risques aussi abstraits et des traitements si peu connus du grand public, il est essentiel de les considérer, entre autres, sur la base d'exemples concrets, et de prendre le temps de procéder à une subsomption aussi précise que possible afin d'étayer les raisons pour lesquelles le cadre actuel est en effet (très) lacunaire. Ainsi, cette

1024 MARTENET, art. 35 Cst., N 96 ; pour une conclusion similaire par rapport au cadre prévu en droit européen, notamment par rapport au droit fondamental à la protection des données à caractère personnel consacré dans la Charte, voir FABBRINI, p. 22.

1025 À ce titre, le rapport d'*AlgorithmWatch* est très clair : « Les déclarations de principe sans propositions concrètes y relatives dominent le paysage [du *People Analytics*] (*statements of principle without concrete guidance dominate the landscape [regarding People Analytics]*) », voir AlgorithmWatch, p. 38.

contribution avait pour but d'analyser le cadre légal qui régit l'un des multiples nouveaux traitements de données automatisés effectués de plus en plus fréquemment dans le cadre de la numérisation du monde du travail. Plus précisément, il s'agissait de savoir si un employeur peut effectuer un profilage des candidats et, le cas échéant, quelles étaient les limites imposées à ce traitement de données par le droit actuellement en vigueur. Dans ce cadre on pouvait également se demander si les dispositions pertinentes protègent les droits des candidats de manière efficace.

Si le profilage au stade de la procédure d'embauche semble être contraire à plusieurs dispositions fédérales et donc illicite, force est de constater que les limites légales imposées à l'employeur doivent être précisées. Cela étant, vu le cadre légal vague et les conséquences (presque) inexistantes en cas d'un tel traitement de données qualifié d'illicite, un employeur peut être tenté de procéder à un profilage.

Plus précisément, on retiendra que si l'art. 328 CO permet la consécration d'une protection de la personnalité à la lumière des droits fondamentaux en constante évolution, il n'est pas certain que cette disposition s'applique également au stade de la procédure d'embauche. L'art. 328b CO, quant à lui, a précisément pour but d'encadrer les traitements de données effectués dans le cadre des procédures d'embauche. Or, cette disposition ne prévoit que quelques limites assez vagues par rapport aux nouveaux traitements de données mis à disposition des employeurs. La LPD, même révisée, soulève de nombreuses questions quant aux nouveaux traitements de données automatisés, comme p. ex. le profilage. En effet, tant les deux définitions du profilage consacrées lors de la révision que le respect de divers principes généraux et la portée des motifs justificatifs ne semblent pas encadrer le profilage de manière précise. Les voies de recours disponibles n'ont pas été améliorées, et les pouvoirs supplémentaires octroyés à l'autorité de surveillance n'auront, très probablement, qu'une portée modeste en pratique. Les autres dispositifs analysés ne sont soit pas applicables au cas d'espèce (LHand, LTr) soit que peu efficaces en raison de leur champ d'application restreint (LEg, LAGH, CP).

Le droit à l'autodétermination en matière informationnelle en vertu de l'art. 13 al. 2 Cst. consacre une obligation positive à l'encontre des autorités publiques qui implique que ces dernières doivent, entre autres, œuvrer à la réalisation de ce droit entre particuliers. La LPD poursuit ce but. Plusieurs rapports publiés soit en doctrine soit par les autorités fédérales elles-mêmes ont à maintes reprises réitéré la nécessité de mieux encadrer les potentielles mesures de surveillance sur le lieu de travail. Or, comme mentionné ci-dessus, les lois fédérales ne parviennent pas à réaliser cette obligation positive de manière satisfaisante. En bref, force est de constater que le Législateur ne saurait se

cacher plus longtemps derrière la LPD révisée en estimant qu'il a suffisamment œuvré à la réalisation des droits qui découlent de l'art. 13 al. 2 Cst. entre particuliers. Ainsi, au niveau suisse, plusieurs révisions du cadre légal doivent être envisagées afin d'améliorer la protection des droits des candidats et offrir une meilleure prévisibilité juridique aux employeurs, qui souhaitent recourir au profilage. Au-delà d'une réévaluation du modèle d'affaires qui sous-tend le secteur économique analysé, on pensera avant tout à la mise en place de mesures sectorielles.

À moyen terme cependant, les défis liés à la numérisation pourront uniquement être adressés si un changement de paradigme a lieu en Suisse, notamment au sein du pouvoir législatif. Afin d'éviter une crise de confiance similaire à celle qui a été engendrée par le scandale des fiches, il est essentiel de rendre les nouveaux traitements de données plus transparents. Si certains efforts ont déjà été déployés, notamment au niveau de l'éducation des plus jeunes, ceux-ci sont insuffisants. La sécurité juridique nécessaire au bon développement de nouvelles technologies et une protection plus efficace des droits des personnes concernées par les nouveaux traitements de données ne sauraient être garanties par l'adoption de définitions sans régime juridique correspondant et la mise en place d'obligations administratives à charge des responsables de traitement dont le non-respect n'entraîne actuellement aucune conséquence juridique. La numérisation du lieu de travail appelle un débat nuancé, qui devrait aboutir à l'adoption de règles (sectorielles) accessibles au responsable du traitement moyen.

Au niveau international, les travaux du Conseil de l'Europe doivent être poursuivis, voire encouragés. La Cour EDH doit cependant encore être sensibilisée aux risques engendrés par les différentes formes de surveillance mises en place par des particuliers. En effet, s'il est vrai que la Cour EDH a reconnu un droit à la protection des données sur la base de l'art. 8 CEDH et qu'elle en a fait découler certaines obligations positives, notamment dans le cadre de litiges survenus sur le lieu de travail, elle n'a ni consacré un droit à l'autodétermination en matière informationnelle indépendant du droit fondamental au respect de la vie privée et familiale, ni fixé une quelconque définition du profilage, de la décision individuelle automatisée ou de l'intelligence artificielle dans sa jurisprudence. Ainsi, il est à espérer que lorsque les juges de Strasbourg seront saisis d'une affaire soulevant de nouvelles questions en matière de protection des données, ils collaborent étroitement avec le Comité des Ministres et sachent profiter de l'expertise avérée de cet organe du Conseil de l'Europe.

Si la présente contribution se limite à une analyse juridique d'une relation précontractuelle bien précise, d'autres relations juridiques sont également concernées par l'évolution rapide des nouveaux traitements de données. Même

s'il est vrai qu'au regard du cadre lacunaire récemment mis en place par le pouvoir législatif, les juges risquent d'être les premiers à devoir intervenir en la matière, les réponses que nos sociétés souhaitent donner aux nouvelles questions liées à la numérisation ne sauraient être l'affaire du seul pouvoir judiciaire. La mise en place d'un cadre légal, social, économique et technique respectueux des valeurs démocratiques doit être, en effet, l'affaire de tous.

Tabelle comparative aLPD/LPD

Contenu	Disposition aLPD	Disposition LPD	Modifications
Déf. données personnelles	Art. 3 let. a	Art. 5 let. a	oui
Déf. personne concernée	Art. 3 let. b	Art. 5 let. b	oui
Déf. données personnelles sensibles	Art. 3 let. c	Art. 5 let. c	oui
Déf. profil de la personnalité	Art. 3 let. d	—	oui
Déf. traitement	Art. 3 let. e	Art. 5 let. d	oui
Déf. profilage et profilage à risque élevé	—	Art. 5 let. f et g	oui
Déf. décision automatisée	—	Art. 21 al. 1er	oui
Déf. responsable du traitement	Art. 3 let. i	Art. 5 let. j	non (hormis modifications linguistiques)
Déf. principe de la bonne foi	Art. 4 al. 2	Art. 6 al. 2	non
Déf. principe de proportionnalité	Art. 4 al. 2	Art. 6 al. 2	non
Déf. principe de finalité	Art. 4 al. 3	Art. 6 al. 3	non (hormis modifications linguistiques)
Déf. principe de transparence	Art. 4 al. 4	Art. 6 al. 3	non (hormis modifications linguistiques)
Déf. principe d'exactitude	Art. 5	Art. 6 al. 5	oui
Déf. principe de sécurité des données	Art. 7 (et art. 8-12 aOLPD)	Art. 8 (et art. 1-5 OPDo)	oui
Consentement valable	Art. 4 al. 5	Art. 6 al. 6 et 7	oui
Atteinte à la personnalité	Art. 12	Art. 30	oui
Motifs justificatifs	Art. 13	Art. 31	oui
Devoir d'informer	Art. 14	Art. 19-21	oui

Sur l'auteure:
Myriam Christ a obtenu le double diplôme Fribourg/Paris II en 2017. Elle a ensuite été stagiaire pendant six mois à la CEDH auprès de la juge suisse avant d'effectuer un semestre d'échange supplémentaire à l'Université hébraïque de Jérusalem. Après une activité d'assistante à l'Université de Zurich auprès de la chaire de la Professeure Keller, elle a travaillé pendant 18 mois en tant que collaboratrice scientifique auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT). Actuellement, elle suit une formation d'avocate dans le canton de Berne.

La Faculté de droit de l'Université de Zurich a accepté la présente thèse de doctorat le 16 novembre 2022 à la demande de la Professeure Helen Keller (1ère rapporteuse) et de la Professeure Regina Kiener (2e rapporteuse) avec la mention *magna cum laude*.

sui generis est une association consacrée à la promotion du libre accès à la littérat*sui generis* est une association consacrée à la promotion du libre accès à la littérature juridique, aux décisions de justice, aux décisions officielles et aux documents juridiques. Depuis 2014, une revue juridique en libre accès est publiée sous le label *sui generis*. La maison d'édition *sui generis* a été fondée en 2019.

Les ouvrages juridiques qui sont publiés dans cette collection sont mis à la disposition d'un large public et sont publiés à la fois sous forme imprimée et en ligne. La version numérique est accessible librement dans le monde entier (Open Access). Les droits d'auteur appartiennent aux auteurs ; les œuvres sont publiées sous une licence Creative Commons.

Précédemment publiés dans la collection *sui generis* :

042 – Andreas Wehowsky: **Expedited Procedures in International Commercial Arbitration**
041 – Lukas Valis: **Digitale Ökonomie: Erforderlichkeit sektorspezifischer ex-ante Regulierung?**
040 – Constance Kaempfer: **Les mécanismes de mise en œuvre du droit international par les cantons suisses**
039 – Ruedi Ackermann: **Der Mietvertrag mit mehreren Mietern**
038 – Lukas Hussmann: **International anwendbare Streitgenossenschaftsgerichtsstände**
037 – Nils Reimann: **Foreign Electoral Interference: Normative Implications in Light of International Law, Human Rights, and Democratic Theory**
036 – Jeremias Fellmann: **Das Verbot von extremistischen Organisationen im schweizerischen Recht**
035 – Florent Thouvenin / Eva-Maria Messerle: **Zur Geschichte des Eigengebrauchs im schweizerischen Urheberrecht – Entwicklung, Erkenntnisse, Quellen**
034 – Nora Camenisch: **Journalistische Sorgfalt: Rechtliche und medienethische Anforderungen**
033 – Joséphine Boillat / Stéphane Werly: **20 ans de la transparence à Genève**
032 – Nicolas Leu: **Kritik der objektiven Zurechnung**
031 – Martin Klingler: **Füllung der Gesetzeslücken im schweizerischen Adhäsionsverfahren**
030 – Christoph Mettler: **Der Anscheinsbeweis im schweizerischen Zivilprozess**

029 – Simone Walser / Nora Markwalder / Martin Killias: Tötungsdelikte in der Schweiz von 1990 bis 2014
028 – APARIUZ XXIII: Recht in der Krise
027 – Maja Łysienia: Seeking Convergence?
026 – Marc Thommen: Introduction to Swiss Law (2nd edition, 2022)
025 – Severin Meier: Indeterminacy of International Law?
024 – Marina Piolino: Die Staatsunabhängigkeit der Medien
023 – Reto Pfeiffer: Vertragliche Rechtsfolge der «Verwendung missbräuchlicher Geschäftsbedingungen» (Artikel 8 UWG)
022 – Nicole Roth: Miteigentum an Grundstücken und einfache Gesellschaft
021 – Roger Plattner: Digitales Verwaltungshandeln
020 – Raphaël Marlétaz: L'harmonisation des lois cantonales d'aide sociale
019 – APARIUZ XXII: Unter Gleichen
018 – Kristin Hoffmann: Kooperative Raumplanung: Handlungsformen und Verfahren
017 – Monika Pfyffer von Altishofen: Ablehnungs- und Umsetzungsraten von Organtransplantationen
016 – Valentin Botteron: Le contrôle des concentrations d'entreprises
015 – Frédéric Erard: Le secret médical
014 – Stephan Bernard: Was ist Strafverteidigung?
013 – Emanuel Bittel: Die Rechnungsstellung im schweizerischen Obligationenrecht
012 – Christoph Hurni / Christian Josi / Lorenz Sieber: Das Verfahren vor dem Berner Kindes- und Erwachsenenschutzgericht
011 – Lorenz Raess: Court Assistance in the Taking of Evidence in International Arbitration
010 – David Henseler: Datenschutz bei drohnengestützter Datenbearbeitung durch Private
009 – Dominik Elser: Die privatisierte Erfüllung staatlicher Aufgabe

Les livres 001 – 008 sont publiés par la maison d'édition *Carl Grossmann*.

Cet ouvrage est publié dans la collection *sui generis,*
éditée par Marc Thommen.

1ère édition 15 novembre 2023

Reproduction de la thèse de doctorat approuvée par la Faculté de droit de l'Université de Zurich.



L'étape de prépresse de cette publication a été soutenue par le Fonds national suisse de la recherche scientifique.

ISBN 978-3-907297-43-8
DOI 10.38107/043
Lectorat : Jean Perrenoud
Graphisme : Müller+Hess, Basel
Imprimerie : Ebner & Spiegel, Ulm

www.suigeneris-verlag.ch

043

LE PROFILA
CADRE D'UN
D'EMBAUCH
PARTICULIE

La nouvelle loi sur la protection des données comprend désormais une définition légale du profilage. La question de savoir dans quelle mesure un profilage effectué dans le cadre d'une procédure d'embauche soumise au droit privé suisse est licite n'a pas encore été abordée en doctrine. Dans le but de combler cette lacune, la présente contribution traite plusieurs questions : le recours au profilage dans le contexte d'une telle procédure d'embauche est-il légal ? Quelles sont les éventuelles limites imposées à l'employeur ? La réglementation actuelle est-elle compatible avec le droit supérieur, notamment avec la Constitution fédérale, la CEDH et le droit constitutionnel européen ? Quelles mesures d'ordre juridique pourraient être mises en œuvre afin de garantir une meilleure protection des droits des candidats ?

sui generis
ISBN 978-3-907297-43-8
DOI 10.38107/043